JPL - 1625-396, Rev. A

P-300

Galileo

Earth Avoidance Study Report

Prepared by:

R. Mitchell

R. T. Mitchell
Earth Avoidance Study Team Leader

Approved by:

M J Cork

M. J. Cork
Launch Approval Engineering Manager
Flight Projects Office

R J Spehalski

R.J. Spehalski
Manager, Galileo Project

November 4, 1988

JPL
Jet Propulsion Laboratory
California Institute of Technology

JPL D-5580, Rev. A

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (cont'd)

Figures

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

SECTION 1

INTRODUCTION

1.1 EARTH AVOIDANCE STUDY OVERVIEW

The 1989 Galileo mission to Jupiter is based on a VEEGA (Venus-Earth-Earth Gravity-Assist) trajectory which uses two flybys of Earth and one of Venus to achieve the necessary energy and shaping to reach Jupiter. These intermediate planetary encounters were not needed on the previous version of the Galileo mission because of the planned use of the Centaur upper stage, which could provide sufficient energy to reach Jupiter on a direct trajectory from Earth. However, after the Challenger accident and the subsequent cancellation of the Centaur as an upper stage for use in the shuttle, it became necessary to design considerably more complex trajectories in order to reach Jupiter with the only remaining upper stage available, the Inertial Upper Stage (IUS). Since the Galileo spacecraft uses radioisotope thermoelectric generators (RTGs) for electrical power, the question arises as to whether there is any chance of an inadvertent atmospheric entry of the spacecraft during either of the two Earth flybys. The purpose of this report is to document a study that has been performed to determine the necessary actions, in both spacecraft and trajectory design as well as in operations, to insure that the probability of such re-entry is made very small, and to provide a quantitative assessment of the probability of re-entry.

In order for the spacecraft to actually enter the Earth's atmosphere during either flyby, a specific sequence of failures and consequences is necessary. First, a spacecraft or ground failure must occur. This failure must cause a velocity change (ΔV) to be applied to the spacecraft, this ΔV must be one that will place the spacecraft on a trajectory that intersects the Earth, and the ability to correct the trajectory must have been lost. A logic diagram showing the possibilities for this sequence of events is indicated in Figure 1-1. Such failure sequences can be classified by whether they occur as a result of a planned trajectory change, i.e., a maneuver, or as occurring even though no course change was planned. The first failure sequence corresponds to following the left branch in Figure 1-1, with an impacting trajectory resulting either from normally occurring statistical navigation dispersions, (which occurs with probability less than 10^{-6}, based on the navigation strategy to be used), or as a consequence of a failure in implementing the maneuver. In either case, a failure that precludes a recovery maneuver is also necessary in order for impact to occur. The second classification of failure sequences corresponds to the right branch in Figure 1-1, and covers the case where the spacecraft is in normal quiescent cruise with no planned maneuvers, and a failure happens which not only causes a ΔV to occur, but also produces a ΔV of magnitude and direction such that an impacting trajectory results. As before, in order for such a failure to cause an actual impact, it is necessary for either this failure or a subsequent failure to preclude the performance of a recovery maneuver. A detailed analysis has been completed which characterizes all such failures, along with their associated probabilities and consequences. These results have then been used to develop a navigation strategy for delivery of the spacecraft to each Earth flyby such that the vulnerability of impact to these failures is made very small and, in some cases, eliminated entirely. The results of this effort are documented in the following sections of this report.

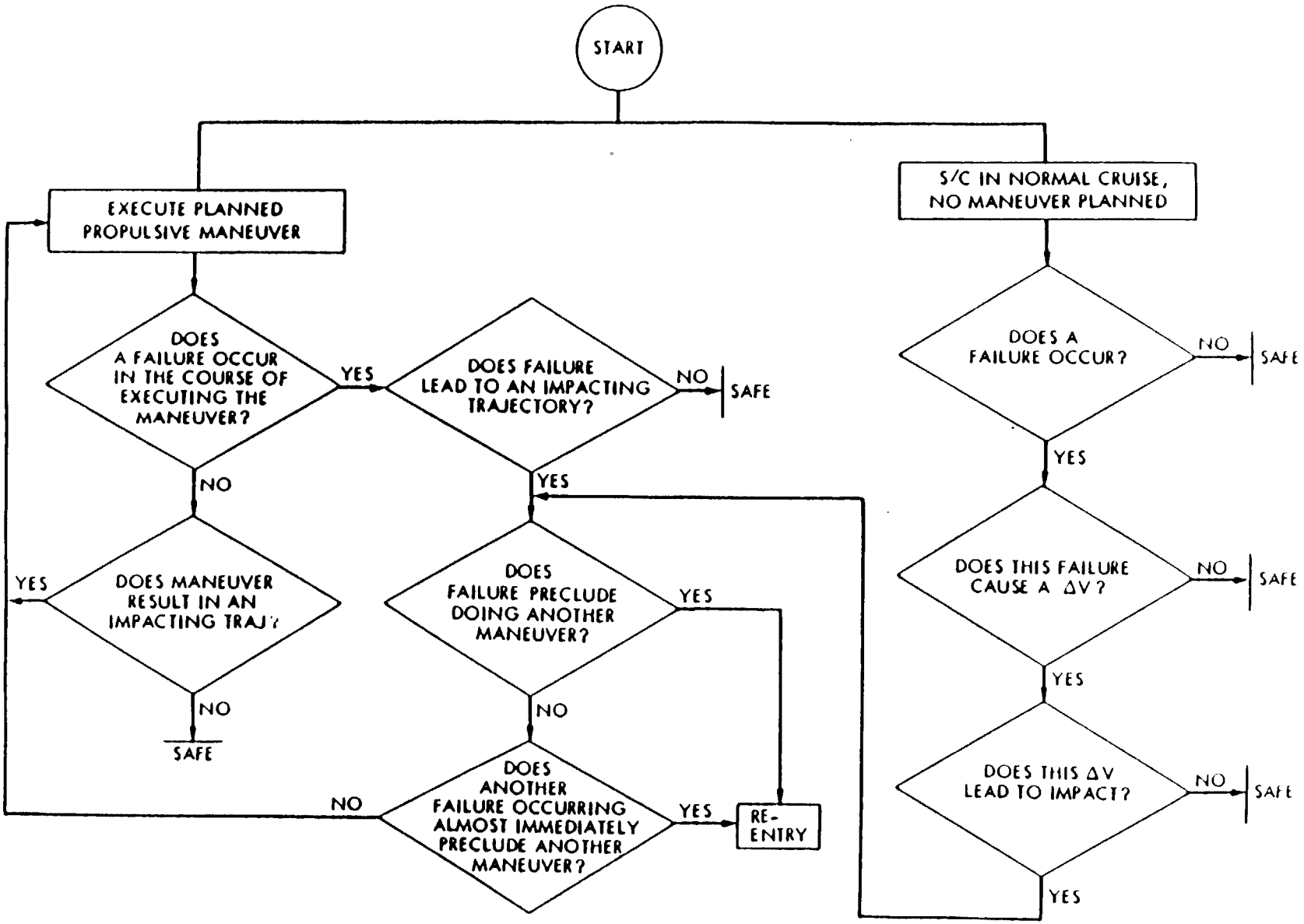


Figure 1-1. Logic Diagram of Sequence of Events Necessary for Re-entry to Occur

1.2 Organization of the Report

The material in Section 1.3 provides a concise summary of the overall Earth Avoidance study, the factors considered, the manner in which the mission is to be flown from launch through the time of the second Earth flyby, and the results. The recommended approach to reading this report, for both the reader looking for a quick overview as well as the reader planning a detailed perusal, is to read this summary before going into the more detailed technical material of Sections 2, 3, and 4 and the Appendix.

Section 2 contains overview material on mission design, navigation, sequencing, and the spacecraft, with particular emphasis on how each of these areas relates to the overall issue of inadvertent entry. This material is primarily intended as background information for the reader not familiar with the Galileo Project, and generally does not describe work done specifically in support of the Earth avoidance study.

A summary of the analysis of spacecraft failure modes is contained in Section 3, and a detailed and highly technical description of the analysis is contained in the Appendix at the end of this report. Specifically, the Appendix material covers the identification of failures that could cause a ΔV to occur, the causes of such failures, and the consequences and possible recovery options if, in fact, such a failure causes an Earth impacting trajectory to occur. The velocity changes occurring as a result of such failures are categorized in terms of their range of magnitude and direction. Probability values are assigned to each failure mode, both in terms of such a failure occurring, and its conditional probability as a function of time along the trajectory.

Section 4 describes the overall plan for navigating the spacecraft past the Earth. A trajectory design strategy is developed using the spacecraft data of Section 3 and the Appendix in such a way as to reduce, and in some cases eliminate entirely, the vulnerability of the trajectory to inadvertent entry as a consequence of potential spacecraft and ground failures. The total probability of entry is developed, including contributions due to normally occurring navigation delivery dispersions, as well as potential spacecraft and ground failures.

This report does not cover the case of re-entry as a result of failures during the launch phase or the on-orbit IUS operations phase of the mission. It also does not report on the breakup analysis for an entry occurring either during launch or at one of the Earth flybys. These potential failure modes and consequences are analyzed and discussed in the NSTS Data Book and the Galileo Final Safety Analysis Report prepared by the DOE.

1.3 SUMMARY OF THE EARTH AVOIDANCE STUDY RESULTS

This Section provides a summary of the analyses conducted and the results achieved in the Earth Avoidance Study. It is intended to provide a non-technical overview of the report, as well as providing a useful starting place for the reader intending to pursue specific areas in depth. Frequent references are made to areas in the report where a specific topic is discussed in detail.

1.3.1 Terminology

Throughout this report, the terminology is used that "impact" refers to a re-entry of the spacecraft into the Earth's atmosphere and "an impacting trajectory" refers to a trajectory that would result in impact if it were allowed to propagate uncorrected. However, the spacecraft, while on an impacting trajectory, may have from days to years to go before impact would occur, during which time corrective action can be taken to avoid impact.

1.3.2 Results

As mentioned previously, there are only two ways for impact to occur during either of the two flybys. The first of these is for a statistical dispersion in the navigation process to lead to an impacting trajectory, followed by either a failure to correctly identify the situation or the inability to take the necessary corrective action. The second way is for a failure to occur, either in ground operations or on the spacecraft, that causes a velocity change to be imparted to the spacecraft that, in fact, places the spacecraft on an Earth impacting trajectory. This must then also be followed by either failing to correctly identify the outcome of the failure or an inability to take corrective action.

The orbit estimation accuracy capability as a function of time described in Section 2, combined with the biased trajectory strategy described in Section 4, shows that at any time in the trajectory the uncertainty in where the current trajectory would pass by the Earth is many times smaller than the planned miss distance at that time in the trajectory. Hence, there can never be any risk of failing to properly identify an impacting trajectory if one actually existed at any time in the mission. Any trajectory that was determined to be passing sufficiently near to the Earth that there was some question as to whether it was on an impacting trajectory would necessarily be well off from the planned trajectory at that time in the mission, and the same corrective action would be taken as though it were clearly identified as being on an impacting trajectory.

The spacecraft failure analysis of Section 3, and the navigation strategy developed in Section 4 based on the spacecraft analysis, have led to the result that the total probability over both Earth encounters that a spacecraft or ground failure will cause a velocity perturbation to the spacecraft, that this perturbation will result in an impacting trajectory, and that a corrective maneuver will not be successfully performed, is 5×10^{-7}.

The navigation strategy has also been developed such that at any time a trajectory correction maneuver is performed, the a priori probability that this maneuver will result in an impacting trajectory is less than 10^{-6}. Then, considering the probability of being able to implement a corrective maneuver, given that an impacting trajectory has resulted, and using the probability of recovery values of Table 3.1, the overall probability of impact occurring as a result of navigation dispersions is so small that it makes no contribution to the total probability when combined with the value of 5×10^{-7} from ground operations errors and spacecraft failures of the last paragraph.

Hence, the total probability of impact, the sum of the probability due to navigation dispersions and the probability due to spacecraft and ground failures, is 5×10^{-7}.

1.3.3 Assessment of the Results

There are places in this analysis where probability values required for events, failures, human error rates, etc., were based on previous experience with interplanetary flights, a knowledge of design and test experience, and an engineering evaluation of how the different systems can reasonably be expected to perform. Since this approach requires somewhat subjective judgement, it was useful to understand how sensitive the final result was to variations in values determined in this manner. The most important area where this approach was used was in the specification of the probability of a subsystem failing at some time over the life of the mission. This influenced both the failure probabilities used in some cases as well as the probability of being able to perform a recovery maneuver, given that a failure had occurred that led to a recovery maneuver being required. The analysis that was done to evaluate this is described in more detail below as well as in Section 4. It is demonstrated in chapter 4 that the final result is not overly sensitive to the values used for the probability of subsystem failure. Considering this and the inherent conservatism in the analysis, the total probability of impact quoted above and derived in Section 4 is considered a "best estimate" upper bound on the actual probability of impact.

To elaborate on how sensitive the answer might be to various of the model assumptions, note, as shown in Section 4, that over 70% of the total probability comes from a failure due to a micrometeoroid puncture of the propellant tanks. This probability determination was based in part on the following assumptions:

(1) The fluence model for cometary micrometeoroids used by Galileo was deliberately made conservative relative to the standard NASA model (see description in the Appendix).

(2) Asteroidal micrometeoroids were included in determining the biasing strategy and the probability of a tank puncture, even though there exist expert opinions to the effect that this source does not exist.

(3) The threshold of micrometeoroid mass and velocity that would cause a tank failure was calculated using models known to be conservative.

(4) The probability of recovery from a micrometeoroid induced failure has been taken to be zero, although in fact, depending on the specific failure that occurs, there is some prospect of implementing a recovery maneuver to avoid Earth impact. Note also that this means that the values used for recovery probabilities do not influence the probability of impact calculations for micrometeoroid-induced failures.

When the analysis was repeated using the NASA cometary model and eliminating the asteroidal model, and keeping all other parameters the same, the probability of impact due to micrometeoroids went from 3.7×10^{-7} to 1.3×10^{-7}.

The approach taken to the problem of assigning values to subsystem failure probabilities was to assign the Project design goal value of 0.01 as the probability that any half subsystem would fail over the eight year life of the mission. The probability of recovery values of Table 3.1 were derived using this value. The assumption that this goal was met is an engineering judgement based on the fact that all subsystems have been very carefully designed, tested, and analyzed, both as subsystems and as part of the overall spacecraft system functional and environmental testing. Then, as a check on the reasonableness of this assumption, part failure rate data for the two Voyager spacecraft was applied to the appropriate Galileo parts, and the corresponding predicted failure rate determined. (The Voyager failure rates, even though based on spacecraft built and launched over 10 years ago, are the most recent available empirical data source for estimating spacecraft failure rates.) Based on these data, a probability of about 5% for half subsystem failures on Galileo was calculated. The analysis for all non-micrometeoroid failures was repeated using this higher failure rate, and the impact probability only increased from 1.4×10^{-7} to 3.8×10^{-7}. Given 1) the technical advances incorporated in the Galileo spacecraft parts relative to those used in the Voyager spacecraft, 2) the greater amount of part reliability analysis and design efforts performed on Galileo, and 3) the considerably greater pre-launch test time on Galileo, JPL concluded that the 1% subsystem failure rate was appropriate for the baseline.

The results of this sensitivity analysis are summarized in Table 1.1. The micrometeoroid probability is bounded by 1.3×10^{-7} and 3.7×10^{-7}, depending on the model used as discussed above. The other failures result in probabilities of impact ranging from 1.4×10^{-7} to 3.8×10^{-7}. In considering the combined effects, it has been concluded that the sum of the baseline values stated (3.7×10^{-7} for micrometeoroids and 1.4×10^{-7} for all other failures) is a proper estimate for an upper bound, given the conservative assumptions used in calculating the effects of the non-micrometeoroid failures, as well as the conservatism in the micrometeoroid model.

Table 1.1. Sensitivity Analysis Results

	Probability of Earth Impact		
Risk Source	Minimum	Baseline	Maximum
Micrometeoroids	1.3×10^{-7}	3.7×10^{-7}	3.7×10^{-7}
All others	$<1 \times 10^{-7}$	1.4×10^{-7}	3.8×10^{-7}
Total		5×10^{-7}	

1.3.4 Navigation Strategy

A navigation strategy has been developed which is to be implemented in-flight from the time of launch through the second Earth flyby to insure that the risk of Earth impact due to both navigation activities and spacecraft and ground failures is kept very small. The basis of this strategy is a trajectory design which insures that for the time period between launch and the second flyby, exclusive of the sixty day period prior to each encounter, the spacecraft is on a path that misses the Earth by many thousands of kilometers, and for a considerable portion of this time misses by millions of kilometers. Then, beginning at sixty days before each encounter, with improved orbit estimation accuracy and reduced sensitivity to velocity perturbations due to the shortened propagation time, the point at which the trajectory would pass by Earth if left to propagate without further control is gradually moved closer. At sixty days, it is moved in to a few thousand kilometers. At 25 days, it is moved to the final encounter conditions. A final maneuver is scheduled at ten days for the final trajectory control if necessary. At the time of the 25 day maneuver, at a distance of about 20 million km from the Earth, the 99% trajectory control capability at the Earth is about 75 km, and by the time of the ten day maneuver, at about an 8 million km distance, it is down to about 25 km. This strategy results in an increase in the use of spacecraft propellant to remove these biases in the trajectory, but little in the way of increased operational complexity, since many of these maneuvers would have been required in any event as part of the normal navigation process.

Two criteria determine the selection of the size of the miss distance to be built into the trajectory at any point in the mission. One is to insure satisfying the 10^{-6} constraint on navigation activities mentioned earlier, and the second is to keep the risk associated with spacecraft and ground failures very small. Details on how these criteria are met are given in Section 4. A summary is provided here. Any time a maneuver is to be designed and implemented in flight, a constraint region outside of which the probability of an impacting trajectory resulting from the maneuver is less than 10^{-6} is to be determined. This contour then constrains the possible set of target trajectories to those lying outside of it. The determination of this constraint is a routine function of the Navigation Team each time a maneuver is to be done, and is based on all data available at that time, including orbit estimation accuracy performance, the actual trajectory resulting from the last maneuver, etc.

As a further constraint, it is also required that if the maneuver is aborted at any time prior to its completion, the resulting trajectory is to also satisfy the same 10^{-6} constraint. Once the region of acceptable trajectories based on the navigation constraint is determined, the next step is to consider the consequences of potential spacecraft failures that might occur during the cruise period between this maneuver and the next. The velocity perturbations that can result from these potential failures are described in the Appendix. The sensitivity of the trajectory to such perturbations varies with time along the trajectory. Knowing how these sensitivities vary, and what the potential velocity changes are, allows the navigators to select different trajectories at each maneuver time that will reduce the risk associated with each potential failure, and in many cases eliminate the risk altogether.

An example of this is that while the spacecraft is passing within the asteroid belt between the two Earth flybys, its trajectory is designed with a bias such that if a ΔV occurs as a result of a collision with an asteroidal micrometeoroid, in all but the very worst case outcome, the ΔV will not be sufficient to move the trajectory enough to reach the Earth. This bias in the trajectory is not removed until after the spacecraft has exited the region containing asteroidal material. There is no concern, relative to Earth avoidance, about the possibility of the spacecraft encountering any debris which may be orbiting near the asteroid which the spacecraft encounters because, while it is believed that this environment represents very little hazard to the spacecraft, it represents no hazard of Earth impact because of this same bias relative to the Earth that is built into the trajectory. A representative set of targets for a trajectory launched on October 9, 1989, is shown in Section 4. In actual flight, this specific set would not be used, rather the techniques summarized here and developed and described in Section 4 would be used to generate a sequence of aimpoints that meet the criteria in the presence of the prevailing conditions at the time of each maneuver.

The minimum flyby altitude of 300 km occurs at the second Earth encounter. This value was selected prior to the completion of the analysis described in this report as a compromise between the desire to go as low as necessary to minimize the total spacecraft propellant requirement to achieve the trajectory to Jupiter, and the need to insure that there was no risk of Earth impact nor even any risk of passing close enough to the upper atmosphere to cause heating to the spacecraft. The value of 300 km satisfied both these criteria. However, as the spacecraft failure analysis progressed, the idea was raised that perhaps the total probability of impact, which was driven by failures and not normal delivery dispersions, could be reduced by forcing the minimum altitude higher. Further analysis demonstrated this not to be the case.

For failures leading to ΔVs of a few meters per second, the probability of impact is essentially determined by the probability of the failure and the probability of recovery. This is due to the fact that, as a consequence of the trajectory biasing strategy summarized above and described in detail in Section 4, most failures before the 25 day maneuver point do not produce enough velocity change to reach the Earth, and after that point the ability is virtually unaffected by the altitude over a variation of several hundred kilometers. The probability is kept small due to the very short period of vulnerability. On the other hand, the cost of raising the altitude has been determined to be prohibitive. A cost in increased propellant usage equivalent to one to two of the ten satellite encounters in the Jovian tour is associated with each 100 km increase in flyby altitude, the variability being a function of the time of launch within the launch period. As a consequence of these results, it was determined that raising the minimum altitude was neither feasible nor beneficial.

The gravity assist technique to be used at Venus and Earth for the Galileo mission is identical in both concept and implementation to that used in previous JPL missions, including the Mariner X mission to Venus and Mercury and the two Voyager spacecraft to Jupiter, Saturn, and beyond. The fact that the Earth is a "target" for this mission doesn't introduce any different issues, other than the safety issue addressed in this report, because radiometric spacecraft navigation is always done relative to the Earth. Then, when the target body is other than the Earth, the position of the spacecraft

relative to the target is found by determining the vector difference of the spacecraft and target positions relative to the Earth. The navigation process is more accurate when the target is the Earth because there are no errors introduced by uncertainties in the position of the target body, and the radiometric data is more accurate because the range from the spacecraft to the tracking station is shorter.

1.3.5 Spacecraft Failure Modes

A thorough study has been conducted to identify all spacecraft and ground operations failure modes that could result in an anomalous ΔV being applied to the spacecraft prior to the second Earth flyby. Since the spacecraft is never deliberately placed on an impacting trajectory and since the navigation activities will never, with probability less than 10^{-6} per maneuver, place the spacecraft on an impacting trajectory, the only way for an impact to occur is as the result of a spacecraft or ground operations failure. The following set of failures have been identified as those that could cause a ΔV to occur. A detailed analysis of each, including causes, consequences, recovery options, and associated probabilities is provided in the Appendix.

(1) Propulsion system tank failure
(2) Propulsion system thrusters stuck, either open or closed
(3) Thruster failures
(4) On-board computer memory failures
(5) Structural failures
(6) On-board computer programming errors
(7) Off-Sun thermally induced failures
(8) Micrometeoroid impacts on the spacecraft
(9) Radiation, cosmic ray, and SEU effects
(10) Spacecraft charging
(11) Command generation process
(12) Uplink command errors

A summary of the resulting risk of Earth impact due to these potential failure modes is given in Table 1.2.

Table 1.2. Probability of Earth Impact by Failure Mode

Failure Mode	Probability of Impact
Failures Due to Micrometeoroid Impact	3.7×10^{-7}
Thrusters Stuck Open or Shut	6×10^{-9}
Retro-Propulsion Module Overpressure Conditions	3×10^{-9}
Other Spacecraft Failures	1×10^{-9}
Ground Operation Errors	1.3×10^{-7}
Total Probability of Impact	5×10^{-7}

1.3.6 Spacecraft Design Changes

As a result of the spacecraft failure analysis, it was determined that one of the major contributors to the total risk of Earth impact was having a failure that would cause loss of ability to command the spacecraft. This of itself would not be a concern from the standpoint of Earth avoidance since the spacecraft is never left on an impacting trajectory. However, since the spinning spacecraft would maintain its inertial attitude, as it moves around the Sun it would gradually change its pointing direction relative to the Sun. Direct sunlight would cause the propellant tanks to overheat, causing an overpressure condition and eventually a failure. This failure would release pressurized propellant, causing a velocity change to the spacecraft from which no recovery would be possible if an impacting trajectory resulted. As a result of this potential hazard, the spacecraft design was modified to incorporate pressure relief devices to insure that no overpressure condition sufficient to cause tank failure can exist. These valves are designed such that no net velocity change would result from an overpressure venting. Details of the failure analysis and design changes are included in the Appendix.

Once the overpressure concern had been dealt with, the remaining primary contributor to the risk of impact was that due to micrometeoroid impacts. One proposal to reduce this was to increase the amount of shielding blankets used to protect the RPM tanks. This option was analyzed in detail with the conclusion that the current design was optimum. Adding more material incurred a mass penalty for no improvement in the RPM tank protection. As a consequence, the blanket design was left intact.

1.3.7 Operational Guidelines and Constraints

A set of guidelines and constraints has been developed to be applied to the operation of the spacecraft during the approach to each Earth encounter to achieve the highest possible likelihood that no anomalous events will occur, and to insure that the detection of any such events occurs as quickly as possible. These plans are described here. The total probability of impact summarized above and developed in Section 4 was determined without factoring in any additional benefits to be gained from these restrictions, so the operational implementation described here provides an additional margin of safety.

Uninterrupted tracking of the spacecraft by the Deep Space Network (DSN) is to be scheduled for at least 35 consecutive days prior to each encounter. This tracking provides both Doppler data and telemetry. Doppler data will provide quick and certain evidence of any deviation in the spacecraft's trajectory. Telemetry data provides insight to the spacecraft's health and status. Many events or failures that would indicate a propulsive event has occurred or is impending can be seen through the spacecraft data. The purpose of this continuous tracking, in addition to supporting the normal operation and navigation of the spacecraft, is to provide the earliest indication possible of any unplanned events.

After the encounter minus 10 day maneuver to place the spacecraft on its final flyby trajectory, no thruster firings, other than those required for spin maintenance and pointing corrections, are to be performed except as a contingency to protect spacecraft health and maintain the correct trajectory. No propulsive maneuvers are planned, and no dual-spin to all-spin transitions are to be performed.

The spacecraft is nominally Sun-pointed throughout most of the early part of the VEEGA trajectory for thermal control reasons. Limited excursions from this attitude are planned for science, engineering, and navigation purposes. However, from the next to last maneuver at encounter minus 25 days on to closest approach for both Earth flybys, no such excursions are to be permitted. To make such turns requires thruster firings, and this restriction is made to minimize the possibility of a ground or spacecraft failure.

1.3.8 Conclusion

The total probability of the Galileo spacecraft impacting the Earth on either of the two flybys has been determined to be, as a "best estimate" upper bound, 5×10^{-7}. A sensitivity analysis was performed, indicating a range in probabilities for each failure mode, depending on the level of conservatism used in certain key assumptions. All spacecraft or ground operations failures that could lead to a velocity change being imparted to the spacecraft have been identified and analyzed. A navigation strategy, in conjunction with the trajectory design, has been developed which, at the cost of spacecraft propellant, is responsive to the set of failures in reducing the risk of Earth impact to the above value. In addition, operational constraints have been developed and will be implemented to even further reduce any risk.

1.4 ACKNOWLEDGMENTS

This report represents the combined efforts of a large team of people at JPL. The major contributors are acknowledged here. The Mission Design overview was written by Lou D'Amario, the Navigation overview by Bill Kirhofer, the Sequence Process overview by Jim Erickson, and the Spacecraft Overview by John Zipse. The analysis effort summarized in Section 3 and described in detail in the Appendix was led by John Zipse. Key contributors to Section 3 were Bob Gounley, Henry Garrett, Bob Bamford, Mack Dowdy, Darrel Jan, Bob Campbell, Norm Cook, and Jim Clawson. The analysis in Section 4 is primarily the work of Earl Maize. Jeanne Collins provided technical editing and documentation support.

SECTION 2

SYSTEM OVERVIEWS

2.1 MISSION DESIGN OVERVIEW

2.1.1 Trajectory Overview

The baseline trajectory for the Galileo mission is a 1989 VEEGA transfer. As the name implies, the VEEGA trajectory makes use of three gravity-assist planetary flybys between launch from Earth and arrival at Jupiter: one with Venus and two with the Earth. This extensive use of planetary gravity assists dramatically reduces launch energy requirements compared to other Earth-Jupiter transfer modes, and allows the spacecraft to be launched by the shuttle/IUS.

The launch period for the Galileo VEEGA mission extends from October 9, 1989 through November 24, 1989. The arrival date at Jupiter is December 7, 1995. A sample VEEGA trajectory for an October 13, 1989 injection* date and the December 7, 1995 arrival date is shown in Figures 2.1-1 and 2.1-2. Figure 2.1-1 shows the inner-solar system portion of the trajectory from launch through the second Earth flyby, and Figure 2.1-2 shows the entire trajectory to arrival at Jupiter.

This sample VEEGA trajectory begins with launch of the spacecraft on an Earth-Venus transfer with a very low launch energy (C_3 = 17 km^2/s^2), compared to that required for a direct Earth-Jupiter transfer. The Venus gravity-assist (VGA) flyby occurs on February 9, 1990 at an altitude of about 14,700 km. This encounter alters the orbit such that the spacecraft is directed back to the Earth and also adds energy to increase the orbit period to approximately one year with aphelion on the Venus-Earth transfer at about 1.3 AU. Approximately two weeks after VGA, the spacecraft passes through perihelion at about 0.70 AU.

The first Earth gravity-assist (EGA1) flyby, shown in Figure 2.1-3, occurs on December 8, 1990 at an altitude of about 1000 km. This encounter adds considerably more energy to the spacecraft, increasing the orbit period to about two years. Approximately one month after EGA1, the spacecraft passes through a second perihelion at about 0.90 AU. Aphelion of the two-year Earth-Earth transfer occurs at approximately 2.3 AU.

The second Earth gravity-assist (EGA2) flyby, shown in Figure 2.1-4, occurs on December 8, 1992 at an altitude of 300 km and adds the final energy increment to the spacecraft which is required for the transfer to Jupiter. At EGA2, the orbit period is raised to about 5.6 years. The total flight time from Earth to Jupiter is about 6 years.

* "Injection" refers (approximately) to the time of the IUS burn. "Launch" refers to the shuttle liftoff time. The time from launch to injection for nominal deployment is about 8 hours; hence, the distinction is not particularly significant for the purposes of this report.

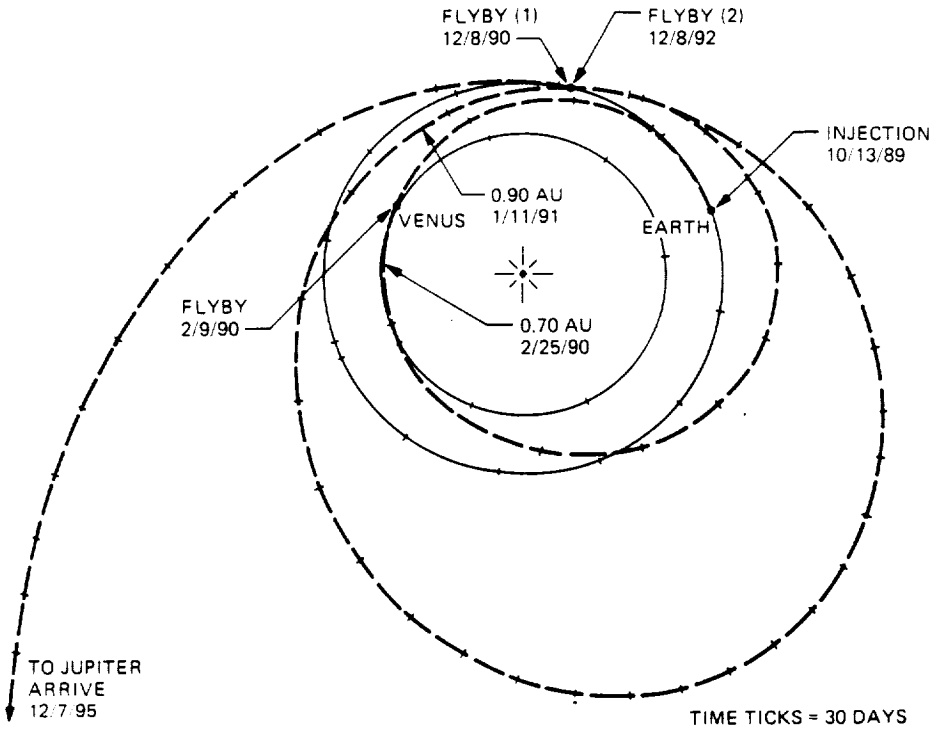


Figure 2.1-1. Close-up of 1989 VEEGA Trajectory Through Earth Flyby #2

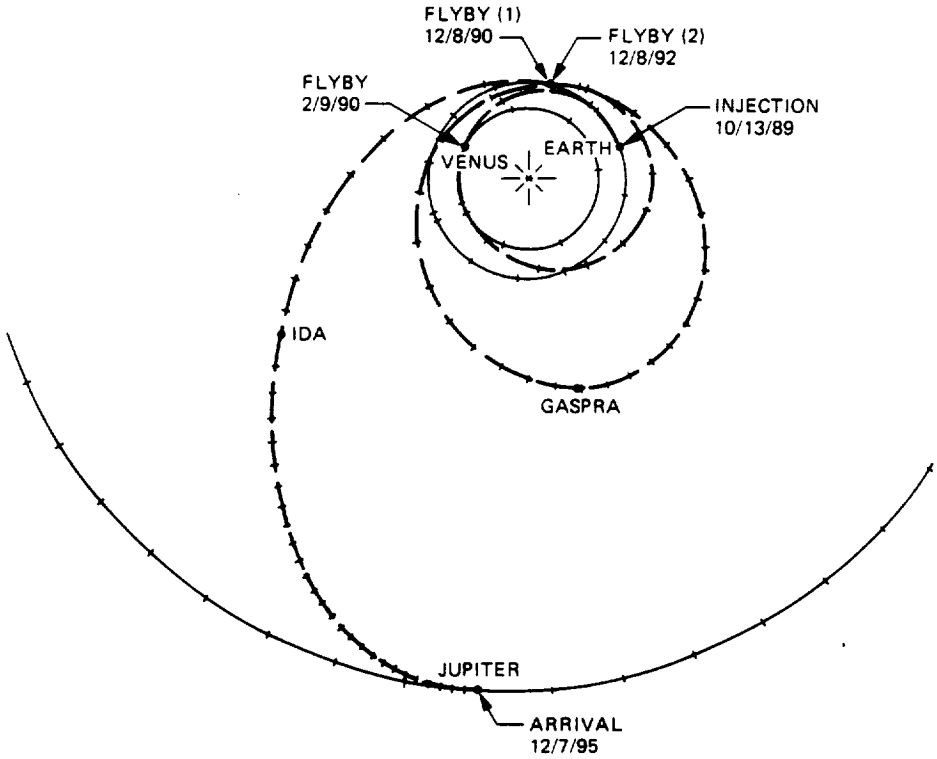


Figure 2.1-2. 1989 VEEGA Trajectory to Jupiter

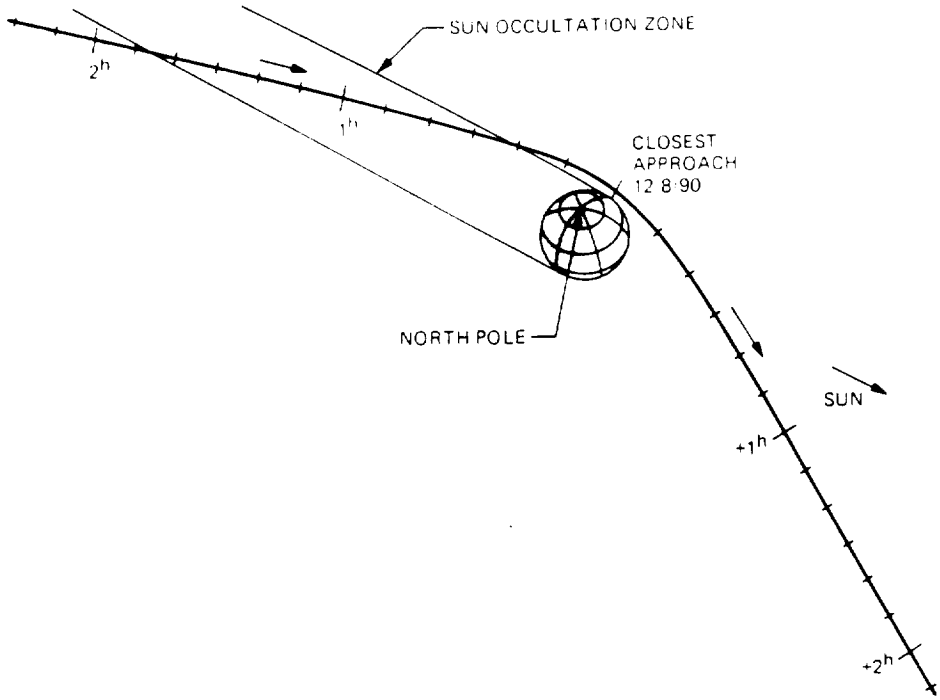


Figure 2.1-3. Earth Flyby #1

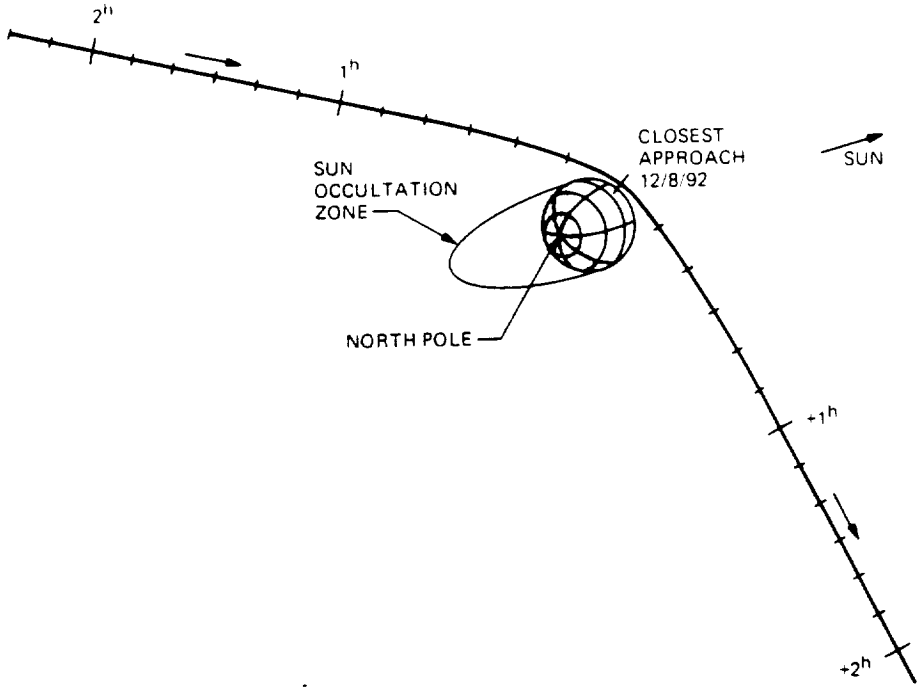


Figure 2.1-4. Earth Flyby #2

2.1.2 Gravity-Assist Concepts

The Galileo VEEGA trajectory utilizes three gravity-assist flybys: VGA, EGA1, and EGA2. The primary effect of these gravity-assist flybys is to reduce the launch energy significantly below that required for a direct Earth-Jupiter transfer. In effect, the spacecraft is being delivered to Jupiter for the launch energy required to go to Venus.

Each of the three gravity-assist flybys adds energy (i.e. velocity) to the spacecraft with respect to the Sun. The manner in which a gravity-assist flyby can increase spacecraft velocity is illustrated by Figure 2.1-5, which shows a "velocity-vector diagram" for EGA1. The spacecraft trajectory with respect to the Earth is a hyperbola; the spacecraft approaches and departs along the asymptotes of this hyperbola at a constant velocity, called the "V-infinity." The angle between the incoming and outgoing asymptotes is referred to as the "bend angle." The velocity vector of the Earth with respect to the Sun at the time of the flyby is indicated on Figure 2.1-5 by the symbol V_E. Adding the incoming and outgoing V-infinities to the velocity of the Earth yields the velocity vectors of the spacecraft with respect to the Sun before and after the flyby.

The effect of the hyperbolic flyby in a planet-centered reference frame is simply to rotate the V-infinity; there is no net energy change for the spacecraft trajectory with respect to the planet as a result of the flyby. However, the rotation of the planet-centered V-infinity has the effect of increasing the magnitude of the velocity vector in a Sun-centered reference

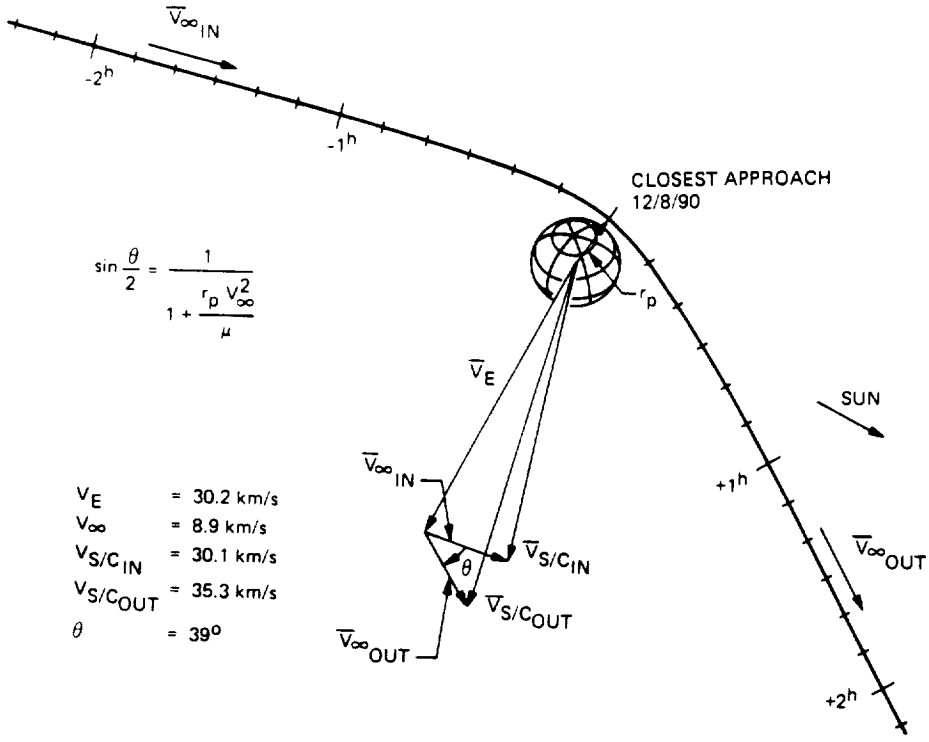


Figure 2.1-5. Gravity-Assist Velocity Vector for Earth Flyby #1

frame. In this example, the Sun-centered velocity has increased from 30.1 km/s to 35.3 km/s, corresponding to an increase in the orbit period from about one year to slightly more than two years.

An important relationship between the radius of closest approach, V-infinity magnitude, and bend angle (a measure of the effectiveness of the gravity assist) is given by the equation shown on Figure 2.1-5. This equation demonstrates a basic fact of gravity-assist theory: namely, that for a fixed V-infinity magnitude, a closer flyby (smaller r_p) will result in a larger rotation of the V-infinity and, hence, a larger change in the Sun-centered velocity. In other words, the effectiveness of a gravity-assist flyby increases as the closest approach distance decreases. Theoretically, the effectiveness of a gravity-assist flyby is limited by the physical radius of the flyby body. Practically, however, the lower limit for the closest approach altitude is dictated by concerns over atmospheric heating effects and impact probability. For the Galileo VEEGA trajectory, the lower limit for the Earth flyby altitude is 300 km.

The 300-km altitude constraint was selected as a value that is low enough to minimize the propellant required for trajectory design and, at the same time, is high enough virtually to guarantee that the spacecraft will not reenter the Earth, and will not even come close enough to experience aerodynamic heating. The 99% delivery errors to the final aimpoint range up to about 25 km, depending on the strategy used for achieving the final aimpoint. This means that at a 300-km targeted altitude, and allowing conservatively 100 km for atmosphere, approximately a 20σ error is required for reentry to occur. In other words, no statistical event will ever lead to reentry; only a failure could do so.

The limitation to the effectiveness of a gravity-assist flyby (due to the flyby altitude constraint discussed above) explains why the VEEGA trajectory requires two Earth flybys. In order for the first Earth flyby to add sufficient energy to the spacecraft to enable it to reach Jupiter, the Sun-centered velocity would have to be increased to about 39.0 km/s. This would require a bend angle for the flyby of about 90° and a corresponding flyby radius of 2100 km, equivalent to an altitude of -4300 km. Allowing a second Earth gravity-assist flyby results in flyby altitudes at or above 300 km for both flybys.

2.1.3 Trajectory Characteristics

The Galileo VEEGA trajectory will be targeted to have one or more close encounters with an asteroid during interplanetary cruise. There are two possible locations for these asteroid flybys: (1) where the spacecraft enters the inner edge of the asteroid belt on the Earth-Earth (EE) leg of the trajectory, and (2) where the spacecraft crosses through the asteroid belt on the Earth-Jupiter (EJ) leg of the trajectory.

The exact strategy of which asteroid(s) will be targeted for each day of the launch period is dictated by spacecraft propellant considerations and has not been decided at this time, although the general characteristics of the strategy are known. For about the first two weeks of the launch period, trajectories will be targeted for a flyby of asteroids 951-Gaspra (EE leg) and

243-Ida (EJ leg). Then the Ida flyby will be eliminated, and trajectories for a range of subsequent launch dates will be targeted only for a Gaspra flyby. Sometime near the middle of the launch period (near the end of October 1989), a switch will be made to trajectories which are targeted only for a flyby of the asteroid 2825-1938 SD1 (EE leg).

The choice of December 7, 1995 as the Jupiter arrival date and the trajectory reshaping necessary to include close asteroid flybys means that all trajectories require one or more small velocity changes provided by the spacecraft propulsion system. Such a velocity change, called a Deep Space Maneuver (DSM), may be located on any one of the following trajectory legs: Venus-Earth (VE), Earth-Earth (EE), and Earth-Jupiter (EJ). In general, the existence of a DSM is linked to either the condition of an Earth flyby altitude being at the 300-km lower limit or the necessity of reshaping the trajectory to include a close asteroid flyby, or both.

In general, optimal trajectories which have flybys of both Gaspra and Ida require a DSM on all three legs. In most cases, the DSM on the EE leg occurs after Gaspra, although early-launch trajectories may have a DSM both before and after Gaspra or the entire DSM may occur before Gaspra. Optimal trajectories with a flyby of Gaspra only behave similarly except that the DSM on the EJ leg is always smaller (because of the elimination of the Ida flyby), and the DSM on the EE leg sometimes has a very small magnitude (< 1 m/s). Optimal trajectories with a flyby of 1938 SD1 generally have only a DSM on the EE leg; this DSM occurs before the 1938 SD1 flyby.

In order to insure that the probability of Earth impact is kept very small, all trajectories will be required to have biased aimpoints until some time prior to both Earth flybys. (The biasing strategy is explained in detail in Section 4.) This requirement means that all trajectories which, without regard for Earth avoidance, do not have a DSM on the VE leg will have to be forced to have a DSM on the VE leg. Therefore, the trajectory will be suboptimal from a propellant utilization viewpoint, although the propellant cost is relatively small. This situation occurs for early-launch Gaspra plus Ida trajectories and for all 1938 SD1 trajectories.

The constant Jupiter arrival date of December 7, 1995 and the constraint of including one or more close asteroid flybys on the trajectory result in little variation in the Earth flyby altitudes. The Earth flyby altitude characteristics for the Galileo VEEGA mission may be summarized simply as follows:

	Earth Flyby Altitude (km)	
Trajectory Type	EGA1	EGA2
Gaspra + Ida	1000	300
Gaspra	1000	300
1938 SD1	4500	300

The EGA1 altitude can vary from the value listed in the above table by $\pm$ 100 km, and the EGA2 altitude can in some cases be slightly greater than 300 km by a few tens of kilometers.

2.2 NAVIGATION OVERVIEW

2.2.1 Introduction

Navigating the Galileo spacecraft safely past the Earth must be insured with great confidence. This purpose is pursued by reviewing the navigation task and relating the history of its performance with the prediction of its capabilities.

Navigation is defined as the process of locating the position and predicting the flight path of the space vehicle and controlling that predicted flight path to achieve mission objectives. A pre-flight mission design activity provides the baseline trajectory for the space flight, from which navigation provides the systems required to execute that flight. Navigation support for each deep space mission involves a planning phase, in which flight accuracies are predicted and the systems to execute the flight are developed, and an operations phase, where the actual process of navigation is executed.

Deep space navigation has experienced an extensive history over the past years. In the 1960's, beginning with the Mariner 2 mission to Venus in 1962, a series of spacecraft was sent to the inner planets to perform remote science sensing during flyby encounters. In the 1970's, the range of navigation applications was expanded to include the delivery of spacecraft to orbit the inner planets; first with the Mariner 9 mission to Mars in 1971, followed by the Viking missions to Mars in 1976, and the Pioneer program to Venus. Finally, in the 1970's the exploration of the outer planets was begun, with the early Pioneers to Jupiter and Saturn, and then with the Voyager program.

The JPL navigation system has evolved over the last 26 years and is currently employed on NASA planetary missions. Section 2.2.2 describes the elements of the measurement system and data processing system that comprise today's navigation system. A summary is provided of the recorded historical performance achieved with the system during the past 26 years of planetary exploration, along with a description of how the system is used operationally. Section 2.2.3 provides a description of the Galileo mission in terms of applying the navigation system to achieve high confidence in the ability to estimate the flight path and, in turn, to navigate the Galileo spacecraft safely past the Earth.

2.2.2 The JPL Navigation System

Figure 2.2-1 illustrates, in schematic form, the elements of measurement and computation that comprise the current JPL navigation system, which is being employed for the Galileo mission. The left-hand side of the diagram shows a spacecraft acquiring optical television images of the target body and being tracked by two ground antennas. On the right-hand side is shown the ground processing system, which models the trajectory motion, estimates the orbit, and computes the flight path corrections.

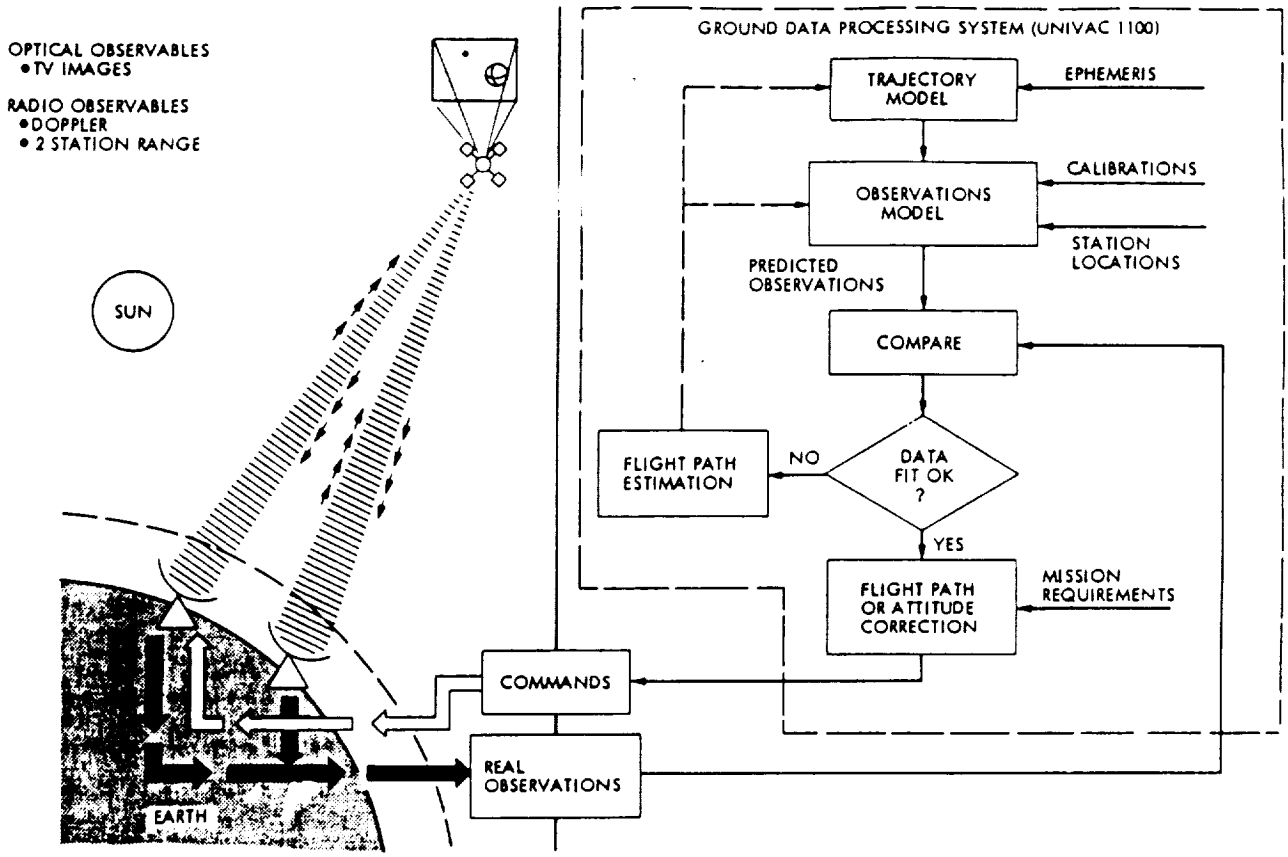


Figure 2.2-1. A Schematic Description of the Current JPL Navigation System Used for Voyager Navigation

2.2.2.1 The Measurement System. The baseline navigation measurement system of the 1960's consisted of two-way S-band (2.3 GHz) radio Doppler. This system was used to navigate the early Mariner missions to Venus and Mars. Beginning with Mariner 9, two-way, 1 MHz bandwidth ranging data were also employed. Ranging data were used as supplementary data to Doppler during the cruise to Mars, and were used as a backup for Doppler during the planet orbiting phase, when the Doppler data noise increased dramatically near superior conjunction. Ranging data, if taken nearly simultaneously from two widely separated stations on Earth, can be used to obtain a direct measurement of the geocentric direction to a spacecraft. Voyager navigation uses ranging data acquired in this near-simultaneous mode.

Beginning with the Viking mission in 1975, NASA spacecraft transponders have transmitted S-band and X-band (8.4 GHz) downlink to Earth, both signals being coherent with the uplink S-band. The processing of S- and X-band data allows a calibration of the effects of charged particles on the downlink signal. Mapping methods are employed to infer the effect on the uplink. This dual frequency technique has been used successfully to calibrate both Doppler and range during periods of high activity in the solar plasma and in Earth's atmosphere.

Optical measurements, acquired from the science cameras onboard the spacecraft, have been used on the Viking and Voyager missions to improve the target relative orbit determination accuracies in the final approach stages of their planet and satellite encounters.

2.2.2.2 The Data Processing System. Doppler, range, and optical image data are brought to the Jet Propulsion Laboratory and buffered on computer tape. A large software system is operated at JPL to determined the spacecraft orbit and compute trajectory correction parameters. The elements of the software system are listed in Table 2.2-1. For each program, the Table provides a short functional description, the size of the program in terms of the approximate number of lines of Fortran code, and the resident computer.

Newly acquired radio data are first processed in the Intermediate Data Records Stripper Processing System (IDRSPS) Program, where the data blocks from different tracking stations are merged into a single time-sequenced array. Data of poor quality are removed from the array in this system and the array made ready in computer storage for the orbit estimation process.

Two modules are used in the orbit estimation process. First, the Double Precision Trajectory (DPTRAJ) system computes an N-body numerical integration of the trajectory and state transition partials from initial conditions. The numerical integration is performed using a variable order predictor, corrector method. The Orbit Determination Program (ODP) computes simulated observables corresponding to each actual observation based on the trajectory "modelled" by DPTRAJ and computes the partial derivatives of the observables with respect to the initial conditions of the trajectory. It may also compute partial derivatives with respect to a multitude of additional trajectory and observation model parameters, such as planet gravity terms, target ephemeris coordinates, spacecraft gas leaks, and tracking station locations. An array of observation residuals is computed and regression analysis is performed to produce a best estimate of corrections to the initial state parameters and the other desired parameters. The product of the process is a numerically integrated trajectory which best fits the observations.

The best estimate trajectory serves as the basis for computation of the velocity correction parameters required to correct the flight path to meet the mission target objectives, a computation which is performed in the Maneuver Operations Program (MOPS).

2.2.2.3 Navigation System Accuracy. Deep space navigation requires the computation of accurate orbits and targeting corrections. These are made possible by the use of submeter accurate modelling throughout the navigation processing system, and the use of several model support systems, which furnish data and constants necessary for accurate computation. Submeter modelling is achieved by the use of double precision (16 decimal digits) in all trajectory and observable computations, and the use of a relativistic light time solution algorithm in the Doppler and range observable computations, which takes into account the retardation in the velocity of light by gravity and the transformation from solar system barycentric coordinate time to Earth station proper time. Model support systems provide the location of planets and natural

Table 2.2-1. Major Software Elements of the JPL Navigation Data Processing System

Program	Function	~ Size (Lines of Fortran Code)	Computer
ODP	Fits data to obtain orbit	200,000	UNIVAC 1100
DPTRAJ	Integrates trajectory	150,000	UNIVAC 1100
MOPS	Computes correction maneuver	60,000	UNIVAC 1100
IDRSPS	Edits and formats radio data	30,000	UNIVAC 1100
MEDIA	Calibrates radio data	30,000	UNIVAC 1100
APP	Plans optical navigation pictures	5,000	VAX 11/780
ONIPS	Extracts optical observable	30,000	VAX 11/780
ONP	Computes optical data partials	15,000	VAX 11/780

satellites in the solar system, the location of the tracking stations on Earth, variations in Earth's rotation and orientation, and the effects of transmission media on the radio signal. A description of these support systems is given here.

(1) The Planetary and Satellite Ephemeris System -- JPL planetary ephemerides are derived primarily from optical transit data, acquired by: the U.S. Naval Observatory over the past century; radar planet surface-bounce range data from the NASA Deep Space Network over the past decade, and spacecraft ranging data from past planetary missions. A large data reduction system, the Solar System Data Processing System (SSDPS) is maintained at JPL to process these many observations and produce the world-standard JPL ephemerides. With the advent of spacecraft ranging data, and with the refinements from lunar laser ranging data, JPL ephemerides for the inner planets and Jupiter are accurate to within 0.2 geocentric microradians. Ephemerides for the planets' natural satellites are developed almost exclusively from astrometric plate measurements and are computed in a data reduction system similar to SSDPS.

(2) Tracking Station Locations -- Position coordinates of the Deep Space Network tracking stations are computed in the ODP itself from Doppler data taken from planetary encounters. The locations of the stations are, therefore, tied to the ephemeris used in the data reduction. As a new planetary ephemeris is generated, so the locations of the Earth tracking stations are recomputed. Stations are located relative to the current ephemeris, to an accuracy of 1 meter perpendicular to the spin axis and longitudinal directions, and within 15 meters along the Earth's spin axis.

(3) Universal Time and Polar Motion -- UT1 and polar motion data are obtained from the Bureau International de l'Heure (BIH) in Paris after its reduction of meridian circle data. These Earth rotation variations are stored in computer files in polynomial form and are applied as calibrations to the computed radio observables.

(4) Transmission Media Effects -- Tropospheric effects on Doppler and range are modelled in equation form. Charged particle effects from the Earth's ionosphere are modelled as elevation-dependent daily varying calibrations, whose values are computed using Faraday rotation data from a NASA Applications Technology Satellite in geosynchronous orbit, the Japanese ETS2 satellite, and the Italian SIRIO satellite. The charged particles in the solar plasma are calibrated directly from analyzing the S- and X-band Doppler data from the spacecraft of interest.

2.2.2.4 Navigation System Operations. The navigation system is operated in support of each deep space mission, both before the actual flight and during the flight. Long before the actual launch, navigation system software is exercised with simulated data. Covariances generated in these exercises enable the analyst to identify the major error sources for the mission of interest and define the total achievable mission accuracy, along with the required measurements and their acquisition schedule. One can also define performance constraints on the spacecraft systems, such as total required propellant or maximum allowable gas leakage rates.

During flight, the navigation system is operated to support the actual guiding of the flight profile. The system produces all of the maneuvers which correct the flight path and furnishes all trajectories used to compute the spacecraft science instrument-pointing sequences and spacecraft antenna-pointing and turning sequences. Doppler data are processed in the navigation system to investigate all spacecraft anomalies, such as abnormal gas leaks, which may affect the flight path. The navigation system predicts the times of all dynamically related mission events, such as occultation times. Finally, reconstructed orbits are used to accurately locate the instrument viewing footprints, which aid the analysis of the science data.

When actual data processing begins, it is conducted as a scientific experiment, in which a hypothesized flight path is adopted and tested against the observations. This testing process is patterned after the pre-flight analysis and is matured well before planetary encounters and usually involves:

1. Computing a multiplicity of flight path solutions, including:

   * Solutions for various radio tracking data arc lengths to examine the distinguishing effect of changing geometry.

   * Solutions for various choices of data types to examine the degree of compatibility or conflict between data types and establish realistic data weighting policies.

   * Solutions for various combinations of estimated parameters to detect mismodelled phenomena and establish corrected model parameter values.

   * Solutions using various data filtering algorithms and a priori statistics on estimated parameters, to detect and compensate for stochastic forces acting on the spacecraft.

   * Solutions using different sets of charged particle data calibration coefficients, to examine the quality and reliability of the different calibration techniques.

   * Solutions with and without the non-gravitational force models derived from attitude limit-cycle data to examine the effectiveness of such models.

2. Computing the expected error covariances of all solutions and their sensitivities to errors in those model parameters which may be difficult to estimate from available data.

3. Selecting an adopted "best-estimate" flight path solution strategy from an in-depth analysis of the following characteristics of all solutions:

   * The noise and signatures in the data residuals,

   * The comparison of the flight path estimates with previous results,

   * The compatibility of model parameter estimated values with estimated values from other sources, and

   * The comparison of computed error covariances and error sensitivities to unestimated model parameter errors and stochastic phenomena.

4. Exercising the adopted strategy to produce the final "best-estimate" flight path.

The computation of maneuvers is also a complex process. It requires the placing of maneuvers at times which are conducive to both minimizing propellant use and achieving high accuracy, and the actual computation of the velocity corrections necessary to reach the desired target. It also requires a strong interaction with the mission management and the often evolving mission goals and policies.

2.2.2.5 Doppler Navigation Performance. One measure of navigation system performance is the statistical accuracy with which navigation delivers a spacecraft to its target. To look at the record of planetary encounter deliveries, it is enlightening to first examine analytically the accuracy which can be achieved from Doppler data received from a station on the Earth, tracking a spacecraft in distant space. This information content can then be compared to actual flight experiences.

On the left half of Figure 2.2-2 is shown a station on the Earth, Doppler tracking a spacecraft at range R, with the Earth rotating at rate W. The Doppler signal is proportional to the spacecraft-station range rate, which follows in time a pattern which closely resembles a sine wave. In the equation within the Figure, we see that the topocentric range rate is approximately equal to the geocentric range rate plus the sinusoidally varying term. The average signal is thus proportional to the geocentric range rate. The amplitude of the sinusoidal term is proportional to the cosine of the geocentric declination.

There are three important points to note concerning the information content of Doppler data in the determination of the position of the spacecraft in the plane perpendicular to the Earth-spacecraft direction (plane of the sky): first, the basic Doppler measurements provide geocentric angle determination, thus the position accuracy of the spacecraft is directly proportional to the geocentric range. Second, the ability of this system to determine declination is inversely related to the sine of the geocentric declination. Therefore, an error in declination is magnified by a factor of the reciprocal of the sine of the declination. This explains the traditional low declination problem often referred to in space navigation literature. Third, the determination of right ascension is not particularly sensitive to variations in geometry. In practice, right ascension is nearly always determined more accurately than is declination. The third dimension along the Earth-spacecraft direction is measured directly very accurately, i.e., <1 km, with the radio metric range data.

An examination of the delivery error record of deep space navigation over the past 26 years requires that the parameters by which performance is judged are carefully chosen. This is because the planetary encounters in the program have occurred at many different geocentric ranges and declinations. Figure 2.2-3 provides an illustration of the Earth relative directions and distances of planetary encounters in the deep space exploration program. Note that Venus encounters generally occurred at geocentric ranges less than one AU, Mars encounters occur outside one AU, and Jupiter and Saturn encounters occur very far from the Earth indeed. Also, note that since all of these encounters have occurred near the ecliptic plane but over a wide range of solar longitudes, the geocentric declinations and right ascensions of the

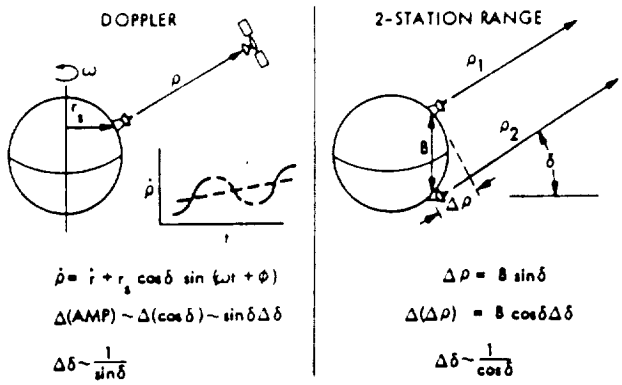


Figure 2.2-2. Properties of Doppler and Range Data as Navigation Measurements

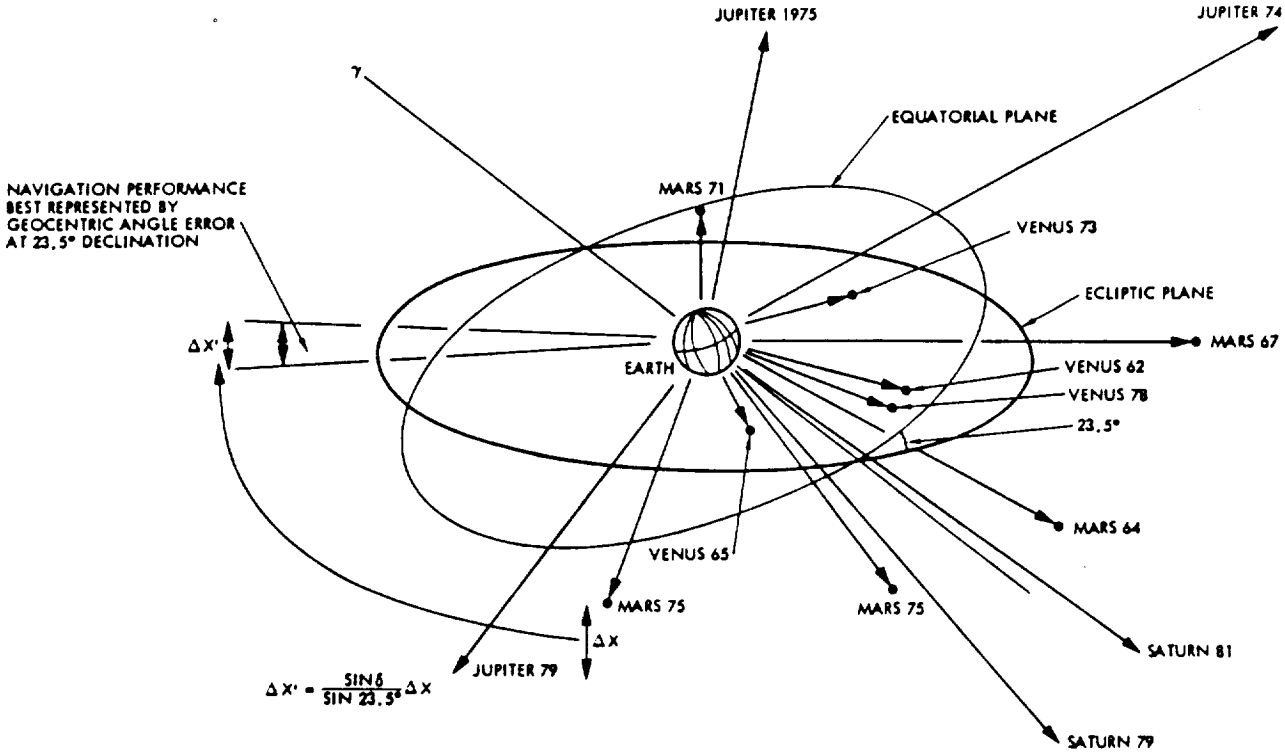


Figure 2.2-3. Geocentric Locations of the Planetary Encounters in NASA's Planetary Exploration Program (1962-1981)

various encounters necessarily differ. Since all these encounters are at various ranges, we must map the range down to some common range like 1 AU. In addition, the comparative navigation performance index for a specific mission might be best represented by the equivalent geocentric declination error at some common declination, such as 23.5 degrees, according to the formula listed in Figure 2.2-3.

Figure 2.2-4 provides the flight record of achievement of deep space radio navigation in terms of the actual delivery error, mapped and adjusted for the differences in declination and range, into equivalent geocentric declination error at 23.5 degrees.

The error values were derived by selecting from the flight records the best or most credible flight path solution based on data obtained before the spacecraft experienced appreciable effects from the gravity field of the encountered planet and subtracting the best, post-flight orbit solution based on data taken during planetary encounter. Since approach trajectory estimates based on data obtained during encounter are extremely accurate due to the effect of gravity on the spacecraft and the Doppler, this difference represents a very good approximation to the actual error in the delivery flight path. The delivery errors for Mariners 2 and 4 were relatively large, but later missions have experienced a remarkable consistency in navigation performance. Note also that Doppler navigation systems have delivered spacecraft to distant targets over the past several years with an accuracy of about 0.25 geocentric microradians (at an equivalent declination of 23.5 degrees).

Note that three mission encounters are missing from the Figure. These are:

1) Mariner 7 at Mars, which experienced small accelerations due to outgassing from a cracked battery case. These accelerations corrupted the Doppler data, precluding accurate reconstruction of the encounter orbit. However, even with this anomaly occurring 5 days before encounter, no significant trajectory change resulted and the previously determined flight path was utilized resulting in a successful encounter.

2) Pioneer multi-probe mission to Venus, which released several probes to Venus then impacted the planet itself, making it difficult to reconstruct an accurate orbit estimate.

3) Voyager 2 at Jupiter, which experienced a failed capacitor in the transponder which adversely affected the Doppler.

2.2.2.6 Two Station Range. An obvious concern develops with the accuracy of Doppler navigation if the target planet is near zero declination when encountered by the spacecraft. Conceptually, a singularity occurs and Doppler orbit determination accuracies in declination fall off sharply. Saturn was at near-zero declination when both Voyager spacecraft encountered the planet. Hence, a new radio metric observation, near simultaneous two-station two-way range, was developed for that mission. If two tracking stations with a long

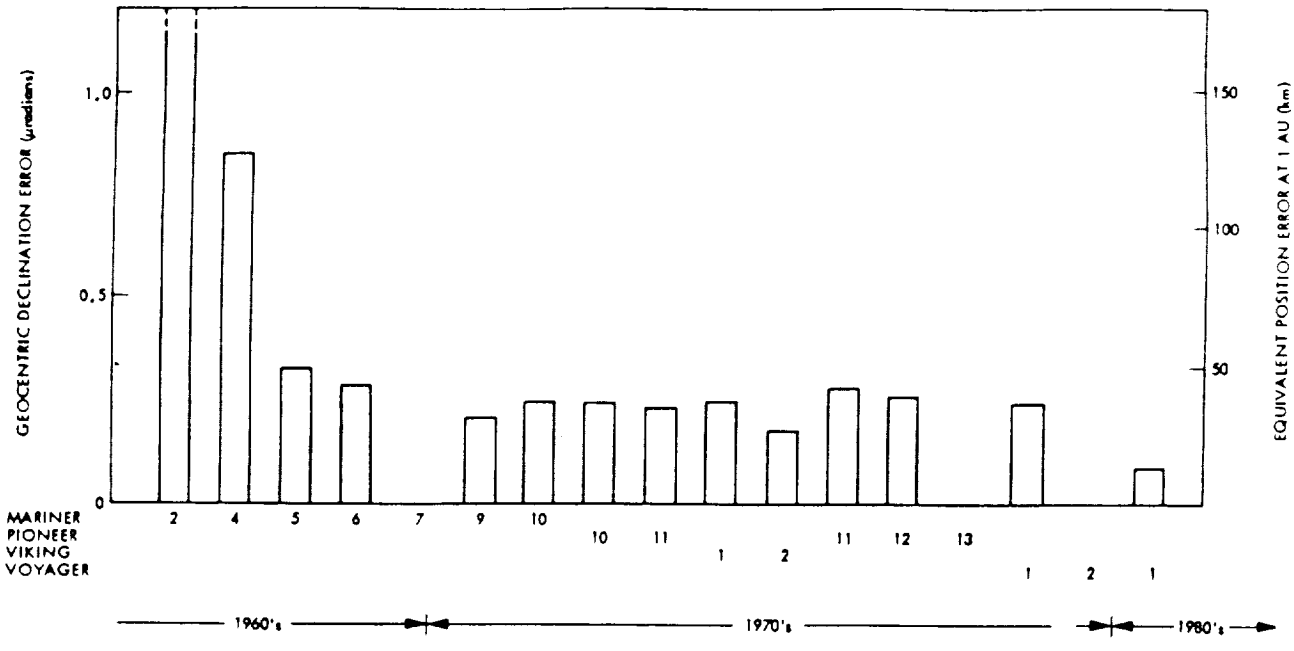


Figure 2.2-4. Mission-to-Mission Doppler Navigation Performance History ~ Equivalent Geocentric Declination Error at δ = 23.5°

north-south baseline, as shown on the right half of Figure 2.2-2, measure the range at almost the same time, errors in the measured range are proportional to the reciprocal of the cosine of the declination, not the reciprocal of the sine. Hence, no singularity occurs at zero declination. The current planetary ranging system produces deep space range measurements accurate to 5 meters; hence, two-station range from stations at California and Australia, with a north-south baseline of 5000 km, can provide a direct measurement of a spacecraft declination accurate to about 1 microradian.

Figure 2.2-5 illustrates, in schematic form, the approximate navigation accuracy which is inherent in the current JPL deep space radio navigation system. The performance possible with Doppler is illustrated by the curved line which approaches an error of 0.25 microradian for high declinations, but falls off to large errors for low declinations. The near-simultaneous range measurement provides a 1 microradian "safety valve" at low declinations.

2.2.3 Orbit Knowledge Determination for Earth Flybys

In support of each Earth flyby, a covariance analysis was conducted to determine the accuracy to which the spacecraft's state is known as a function of time. Results for each flyby are based on the spacecraft tracking schedule, which acquires two tracks of coherent S-band Doppler data per week during cruise, and continuous Doppler within ten days of spacecraft maneuvers. One range measurement is contained in each Doppler track. Each covariance was developed using techniques and error source models which have been proven by past experiences of flight projects to be valid.

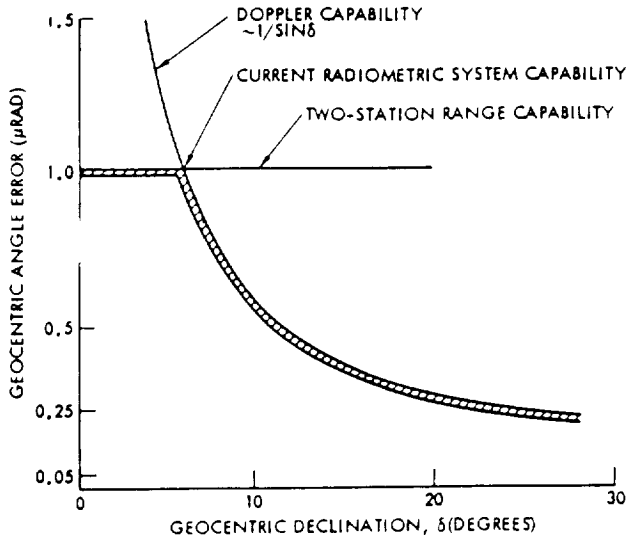


Figure 2.2-5. The Geocentric Performance of the Current JPL Radio Navigation System

In the analysis of each flyby, knowledge of the spacecraft's state was derived as a function of time, as were uncertainties in maneuvers, constant and random nongravitational accelerations due to gas leaks, and the component of solar pressure along the Sun-spacecraft line (radial). Incorporated in these derivations are the considered effects of constant errors in tracking station locations, ionosphere, troposphere, Earth's ephemeris, and Earth's gravitational parameter (μ). (Errors sources which are not estimated but yet permitted to influence the covariance are said to be "considered.") State knowledge is expressed in terms of the Earth encounter B-plane where B·T can be thought of as the radial (with respect to Earth) projection of the spacecraft's encounter position onto the ecliptic plane, and B·R is the corresponding projection orthogonal to the ecliptic. In terms of B·T and B·R, Figure 2.2-6 illustrates the knowledge uncertainty of the spacecraft position as a function of time for EGA1. The knowledge profile for EGA2 is similar.

As a means of assessing the sensitivity of the knowledge solution to the major error sources, uncertainties in solar pressure and a constant nongravitational acceleration were not estimated but rather treated as sources of constant errors in the estimation of the spacecraft's state. Table 2.2-2 lists the contributions of the above error sources to uncertainty in knowledge of spacecraft position at 70 and 30 days before EGA1. It is readily seen that solar pressure is a dominant error source. For example, at 70 days prior to EGA1, the assumed 8% error in solar pressure, if not solved for, would contribute 97 km to a total 126 km uncertainty in B·T. The probability of an error of this magnitude remaining undetected after a year of cruise, during which solar incidence conditions vary considerably, is very low. However, even if it were undetected, the contribution of this error source to Earth impact probability is negligible with the biasing strategy described in Section 4.

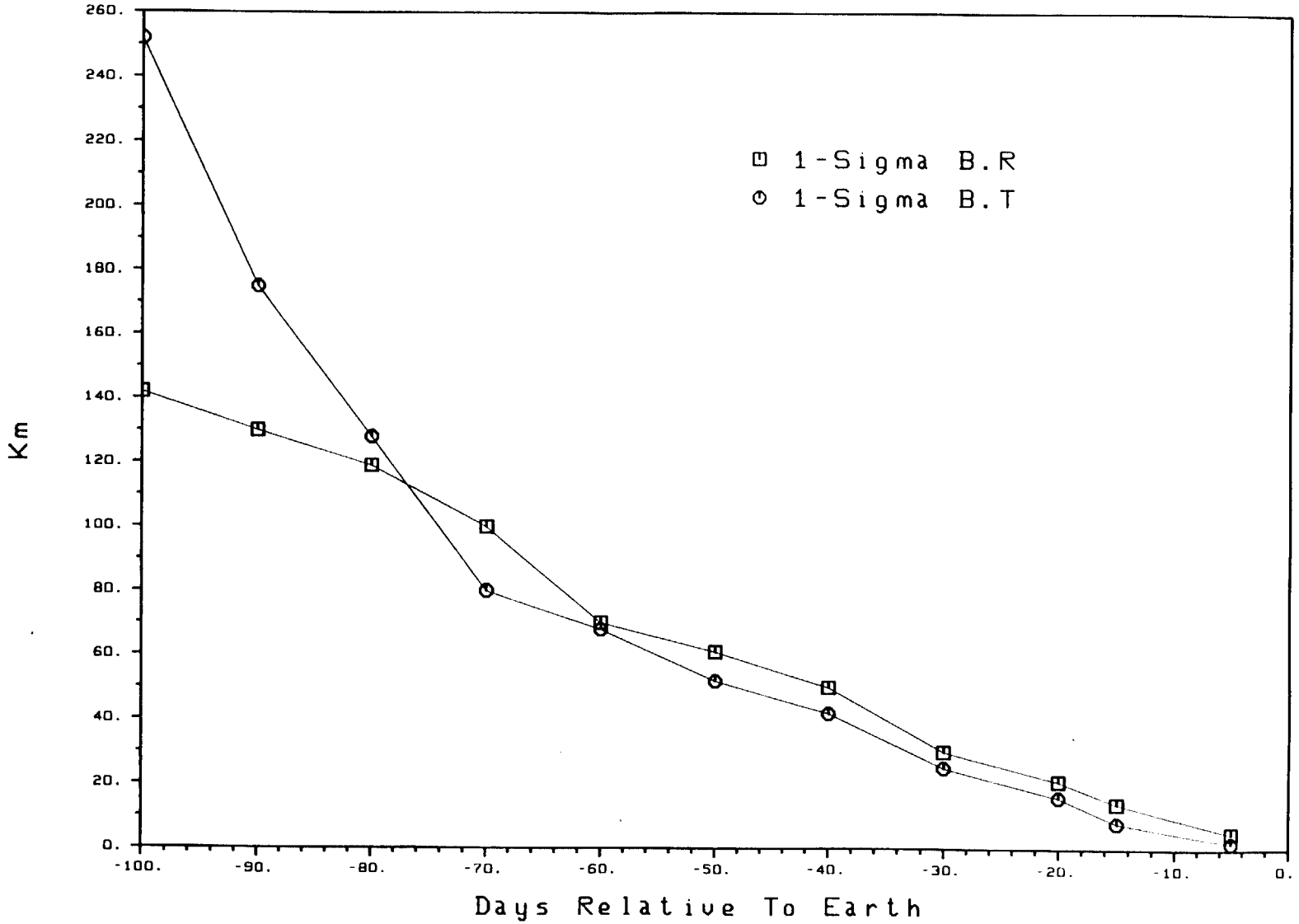


Figure 2.2-6. Spacecraft Knowledge History for EGA1

Table 2.2-2. Major Error Source Contributions to 1-σ Uncertainties in Position Knowledge

Error Source	EGA1 Minus 70 Days B·R (km)	EGA1 Minus 70 Days B·T (km)	EGA1 Minus 30 Days B·R (km)	EGA1 Minus 30 Days B·T (km)
Data Noise	27	47	28	23
Nongrav Accelerations	6	34	5	4
Solar Pressure	43	97	10	12
Ionosphere	71	8	12	4
Troposphere	11	5	1	1
Tracking Station Location	49	43	2	5
Earth Ephemeris	24	34	1	0
Earth μ	0	1	0	0
RSS†	104	126	33	27

†Square root of the sum-of-squares of the error contributions.

It should be noted that the Earth's ephemeris is not a dominant error for the flybys, since Earth is the target, as well as the observing platform.

2.3 SEQUENCE PROCESS OVERVIEW

The sequence process for Galileo takes the basic desires of the Galileo Flight Team (Orbiter Engineering, Probe Engineering, Navigation, Mission Design, and Science Teams), generates the spacecraft commands necessary to achieve them, and causes the correct execution of those commands on the spacecraft.

There are three basic phases to the process:

1) Generating and reviewing the desired activities

2) Translating the activities into the spacecraft commands and validating them, and

3) Executing the commands correctly onboard the spacecraft.

2.3.1 Activity Generation and Review

The process begins with the Mission Design Team (MDT) generating a timeline showing major activities and tracking coverage (a skeleton Cruise or skeleton Orbit Plan). It is a high-level plan for a given spacecraft command

load. The next level of detail shows the science and engineering requests at the activity level. Individual functions such as a UVS observation or pointing correction are identified. These activities define the plans to a level which can be assessed for feasibility, risk, and resource usage (a Cruise or Orbit Plan). The planned activities are then approved by the Mission Director or Project Manager.

At this point, maneuver activities are separated out from all other planned activities, and treated as a special process. A space is reserved in the sequence for the maneuver, while the rest of the sequence is designed and implemented. The maneuver is designed, and commands for it generated later, when more information is available from navigation. However, for understanding the sequencing process, maneuvers can be used as a good example.

The sequencing activity for propulsive maneuvers starts with a set of inputs from the Navigation Team. These inputs are used by the Orbiter Engineering Team (OET) to define a set of parameters that can be executed on the spacecraft. These parameters are then used by the Navigation Team (NAV) to validate the maneuver design.

The next step in this process is for the OET to provide the maneuver parameters to the Sequence Team (SEQ). These parameters are entered into the program set called SEQGEN, internally reviewed by the OET, and then released to the SEQ. This file contains the parameters that will be used to generate the actual command load for the spacecraft.

At this point the Project conducts a Maneuver Design Approval Meeting. This is the meeting in which the Project Manager/Mission Director must review and approve the OET's Engineering Request File. The review covers the navigation design, the OET's implementation, and the NAV maneuver verification. This review is to ensure agreement between the Project and the flight teams as to the design and implementation of all propulsive maneuvers.

2.3.2 Command Generation and Validation

SEQGEN is a set of tested programs that contains expansion and constraint algorithms for all "standard activities." These standard activities are called sequence components, and all maneuvers are designed to use these sequence components. Sequence components are the building blocks of the Galileo sequencing system. They are profile activities (PAs), ground expanded blocks (GEBs), spacecraft expanded blocks (SEBs), and commands. Profile activities are complete functions, such as a continuous slew mosaic or engineering calibration. Ground expanded blocks are algorithms used by several PAs to perform a specific function. Spacecraft expanded blocks are stored onboard the spacecraft and used by PAs. The SEBs are called by a perform command onboard the spacecraft and supplied data by the sequence.

Profile activities have four main sections. The first is called input parameters; these are the variables needed to define a specific activity, examples are turn attitude and burn duration. Next is the relational constraints section which performs internal consistency checks and forces inputs to comply with mission and flight rules. The expansion section is an algorithm that uses the input parameters to generate the time-ordered command list and calls to any SEBs if required for that activity. The checker section combined with SEQGEN checks constraints that are external to the component, examples are downlink and recorder availability. This is also the central program for enforcing mission and flight rules. Each flight and mission rule is assigned to be checked in one or more ways, i.e., ground software or team procedures.

Returning to the process, these parameters are used to generate a time-ordered list of commands and to check many constraints associated with sequencing.

The next step in the process is for the SEQ to produce the detailed products for Flight Team review. This includes the spacecraft sequence file, the spacecraft event file, and SEQTRAN products. The spacecraft sequence file contains the time-tagged set of commands and is read by SEQTRAN to produce the sequence load. The spacecraft event file is generated from the spacecraft sequence file and also contains the time-ordered list of commands, plus additional statements describing the command functions and expected spacecraft events during execution. The SEQTRAN products include the ground command file, which contains the actual data that will be transmitted to the spacecraft, and a human-readable form of the sequence load. The MCT then generates the integrated sequence of events (an integrated listing of spacecraft and ground events) at this time, using the spacecraft event file as input.

When sequence components are used to generate these products, no ground simulation is necessary. This is because of the extensive testing and review each component goes through before use. Each component was thoroughly acceptance tested before delivery to the Project. The next phase of testing was to simulate their execution on the Minimum Capability Hybrid Simulator. This is used to verify the correct execution of a component in the CDS. It verifies that the sequence was correctly translated by SEQTRAN and that the CDS will issue the commands at the correct time. The final phase of testing was executed on the spacecraft during system test. This assures that the spacecraft will perform the activity as planned and designed. During spacecraft testing, an end-to-end verification was accomplished. The spacecraft testing included all types of maneuvers. The test cases were designed for both nominal and fault cases (e.g., burn longer than maximum burn time) of the sequence.

This is the way Galileo plans to perform cruise and orbital operations sequencing, including maneuvers. If a sequence is generated from individual commands or by editing a standard sequence component, then it is required to be validated on the Minimum Capability Hybrid Simulator at this point in the process. This will verify that the CDS issues the commands as required and that the translation was done correctly.

An additional safeguard for all sequences is the restricted command list (all propulsive maneuver commands are on this list). All sequences are searched for any command on the list. This is accomplished using a program called STRIPPER, and the set of commands on this list found in a sequence is delivered with every sequence load. This list of restricted commands is part of the review package delivered to the flight teams. The list must be approved by the OET Chief and the Mission Director.

These products are distributed to the flight teams and the Project Office for review. The Maneuver Command Product Review and Approval Meeting is then held. Here, again, the Mission Director along with the flight team must approve the sequence. This review ensures that the sequence to be sent to the spacecraft accurately represents the maneuver design previously reviewed. All sequences are subject to this level of review.

The process for non-maneuver sequences is similar. Only the names of the reviews and the teams giving inputs are different. The approval of all changes to a sequence rests with the Mission Director.

2.3.3 Spacecraft Execution

Command loads are transmitted as messages. Each message has an error detection and correction code (the code is a shortened BCH). This code allows the correction of any single error and the detection of more than one error. The spacecraft will reject any message with more than one error. Each frame in the uplink message also contains a checksum, which is verified in the hardware command decoder. Each message is assigned a sequential number by SEQTRAN. The spacecraft keeps track of each message as it is received. The last message contains the conditional execute for the load. The load will not become active unless all the messages have been received and accepted by the spacecraft.

Onboard protection for certain types of faults and execution errors is also provided. Before starting a turn, the sequence checks a global variable called SYS1, to ascertain whether or not any one of a set of system faults has occurred. If SYS1 has a bit set, the sequence is terminated. The sequence machine will then wait for new instructions to be uplinked. If there are no system-level faults indicated, the sequence continues.

The sequence checks the status of SYS1 before each segment in a pulsed maneuver and at the completion of each continuous axial burn maneuver (the axial maneuver block sets the thruster branch before the first segment). This is true for vector mode and non-vector mode maneuvers. The response is the same, if a system fault has occurred the sequence is terminated. If no fault is indicated the sequence continues as planned. For continuous axial burns, the nominal termination of the burn is under accelerometer control and for pulsed burns, the number of revolutions. In both cases the sequence has a worst-case burn complete time after which a stop command will be issued to terminate the burn.

An additional constraint is placed on accelerometer-controlled burns, a minimum burn time before which the burn cannot be terminated by the accelerometer. This ensures a minimum burn even if the accelerometer fails.

In addition, a maximum burn time is also specified to insure against an overburn if the accelerometer fails.

The onboard system fault protection has the ability to cancel sequences if needed. Due to the fact that none of the sequenced activities (except launch and relay-JOI) are time critical, the philosophy of cancelling the sequences in the presence of a fault has been adopted. This will result in the sequence virtual machine terminating all sequence activities. The system fault protection will also terminate any maneuver that is occurring.

2.4 SPACECRAFT OVERVIEW

2.4.1 Introduction to the Galileo Spacecraft Design

The Galileo spacecraft (shown in Figure 2.4-1) consists of three major parts. Two parts are the spun and despun sections of the spacecraft which will orbit Jupiter. The third is a Probe which will be released into the Jovian atmosphere.

2.4.1.1 Spacecraft Sections. The spun and despun sections are connected by the Spin Bearing Assembly (SBA), which controls rotation and transmits power and signals between the two sections. The spun section nominally rotates at 3.15 rpm and contains most major engineering subsystems, including the Retro Propulsion Module (RPM), the Radioisotope Thermoelectric Generators, the radio frequency (RF) subsystem and antennas for ground communication, as well as many of the science instruments. A star scanner and Sun sensor are mounted on this section to allow spacecraft attitude determination. The science instruments on the spun section are those which make measurements while continuously sweeping throughout space, as opposed to being pointed in a single direction. The spun section's rotation provides these instruments with a 360° sweep in "clock" angle, while some incorporate internal capability to point in "cone" angle to provide a complete 4π-steradian coverage of space. The spun section instruments are the Magnetometer, Energetic Particle Detector, Plasma, Plasma Wave, Dust Detector, Extreme Ultraviolet, and Heavy Ion Counter subsystems. These instruments will measure and map the Jovian magnetosphere, the Io torus, and the solar wind, and provide insight into their interaction in the vicinity of Jupiter.

The despun section of the spacecraft provides the capability to point a platform of scientific instruments in a fixed direction. The despun section contains only the electronics necessary to its function, since the spun section provides a more evenly cooled housing for the majority of the electronics. The major component of the despun section is the scan platform, which is articulated by the Scan Actuator Subassembly (SAS), to point through 180° of cone angle. The scan platform is also articulated by the SBA which moves the entire despun section through 360° of clock angle. By controlling the SBA and SAS, the scan platform instruments can be pointed in any direction. In addition, the despun section includes gyros and accelerometers for improved platform pointing and spacecraft attitude determination. The science instruments contained on the scan platform are the Solid State Imaging camera, the Near Infrared Mapping Spectrometer, the Ultraviolet Spectrometer, and the Photopolarimeter Radiometer. These instruments provide broad spectral coverage of

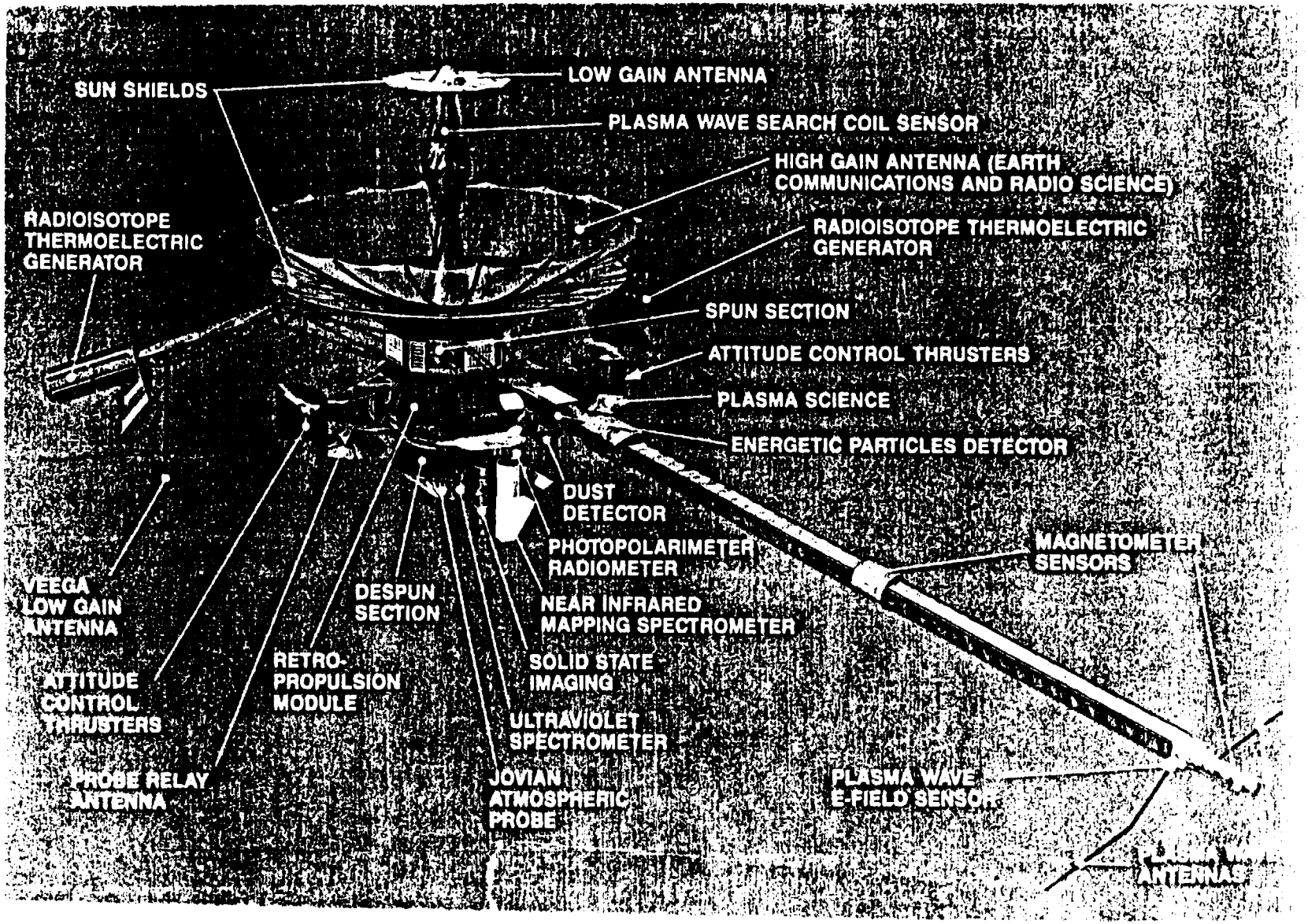


Figure 2.4-1. Galileo Spacecraft

celestial bodies at which the scan platform is pointed and will provide geological and atmospheric data on Jupiter and its moons.

The despun section also carries the Galileo Probe. This instrument package is released about five months before closest approach to Jupiter on a trajectory that will cause it to penetrate the Jovian atmosphere. After entry, the Probe, operating on its own battery, transmits its data back to the Orbiter. The Orbiter receives the data through an articulated antenna and receiver mounted on the despun section and relays it to the Earth. The Probe spends approximately an hour descending through Jupiter's atmosphere and relaying data before the increasing depth causes loss of signal and eventually crushes the Probe. The Probe instruments are designed to measure as much as possible in the upper layers of the atmosphere. They include an Atmospheric Structures Instrument, Neutral Mass Spectrometer, Helium Abundance Detector, Nephelometer (cloud detector), Net Flux Radiometer, and Lightning and Energetic Particle Detector.

2.4.1.2 Spacecraft Modes. The spacecraft is flown in six basic attitude control modes during the mission. First, it is launched in launch mode with the spun and despun sections mechanically locked together so they cannot move relative to one another. Upon release from the shuttle, the spacecraft deploys its booms in deployment mode and unlatches the spun and despun sections. The Spin Bearing Assembly then keeps the two sections stationary relative to one another, both spinning at the nominal spin rate. When all deployments are complete, the spacecraft is placed in all-spin mode, which continues for several days while the spacecraft maintains a nearly Sun-pointed attitude using the Sun sensor.

As the spacecraft subsystems are further verified and calibrated, the spacecraft is eventually commanded to a dual-spin state where the despun section is held fixed in inertial space, the spun section spins at 3.15 rpm, and attitude determination is done primarily using the star scanner (in cruise mode) or the gyros (in inertial mode). Cruise mode will be the mode most often used and is appropriate when neither maneuvers nor precise scan platform pointing is being done. When the spacecraft must turn, the star scanner can no longer provide attitude reference and inertial mode is used. The all-spin-low mode is used to perform 10-newton thruster axial ΔV maneuvers. For these maneuvers, the entire spacecraft is spun at 3.15 rpm.

The final mode is used for two critical events when the spacecraft nears Jupiter. At the time of Probe release, the spacecraft is transitioned to all-spin mode and then spun up to 10.5 rpm for Probe release. This is "all-spin high" mode. It allows for better spin stabilization of the Probe prior to separation. The all-spin high mode is used again about seven days later to provide dynamic stability during the first of the mission's three 400-newton engine maneuvers. This maneuver, the orbit deflection maneuver, adjusts the trajectory so that the spacecraft will overfly Jupiter rather than follow the Probe into the atmosphere. The all-spin high mode is next used for the Jupiter orbit insertion maneuver which occurs shortly after Probe entry and relay and puts the spacecraft into orbit about the planet. About three months later, the final 400-newton engine firing for the perijove raise maneuver adjusts this orbit to keep the spacecraft outside of the most intense regions of the Jovian radiation belts. Thereafter, the spacecraft returns to cruise and inertial modes to conduct the orbital tour of Jupiter and its satellites.

2.4.2 Spacecraft Subsystems

A simplified spacecraft block diagram is shown in Figure 2.4-2 where the major engineering subsystems are highlighted. The spacecraft receives commands and transmits telemetry to the ground through the S/X-band Antenna (SXA) subsystem, the RF Subsystem (RFS), and the Modulation Demodulation Subsystem (MDS). The Command and Data Subsystem (CDS) processes commands and telemetry, executes autonomous programs such as stored sequences and fault protection, and acts as a central interface to the rest of the spacecraft. CDS communicates with all science subsystems, as well as the Attitude and Articulation Control Subsystem (AACS), the Power and Pyro Subsystem (PPS), Data Memory Subsystem (DMS), and the Probe Radio Relay Hardware (RRH). AACS determines spacecraft attitude through several sensors, articulates the despun section and scan platform, and controls the spacecraft attitude by commanding the thrusters in the Retro Propulsion Module (RPM). The PPS controls pyro-actuated spacecraft events and regulates and distributes electric power from the Radioisotope Thermoelectric Generators (RTGs) to the entire spacecraft. The RRH consists of redundant receivers connected to an articulated antenna designed to receive Probe data after entry. A more detailed description of each of these subsystems follows.

2.4.2.1 S/X-Band Antenna Subsystem (SXA). Galileo uses a 4.8-meter-diameter furlable antenna to communicate with Earth. This antenna is similar to the type developed for NASA's Tracking Data Relay Satellites. Due to the extremely high solar flux during the early part of the mission, this High-Gain Antenna (HGA) will not be used and will remain furled behind a Sunshade. During this period and later for redundancy and when the HGA is not Earth pointed, the spacecraft will rely on two wide beam low-gain antennas (LGAs), pointed in opposite directions, one coaligned with the HGA.

Commands are received by the spacecraft primarily on S-band using either the HGA or LGAs. Commands can also be received on X-band via the HGA only. Telemetry is transmitted via X-band through the HGA and via S-band through either the HGA or LGAs.

2.4.2.2 Radio Frequency Subsystem (RFS). Command data are received via an S-band transponder and telemetry is returned to Earth using either a 10/30 watt S-band Traveling Wave Tube Amplifier (TWTA) or a 10/22 watt X-band TWTA. The S-band system can use either the LGAs or HGA while the X-band operates only over the HGA. The S-band transmitter is turned on after separation from the shuttle Orbiter.

The two-channel downlink of the Orbiter is utilized in the following manner. One channel is used for the continuous transmission of fixed-format, low-rate (40 b/s), real-time, uncoded engineering data via S-band. The other channel is used for either real-time or playback data, at data rates between 10 b/s and 134.4 kb/s, via X-band. During the first solar orbit of the mission, only the LGAs will be available for communications until the HGA can be safely deployed and the spacecraft Earth pointed. Furthermore, the spacecraft is usually Sun-pointed until after the second solar orbit for thermal control of the spacecraft, thereby precluding HGA command. The HGA will not be deployed until the spacecraft range to the Sun is large enough to prevent overheating of this antenna.

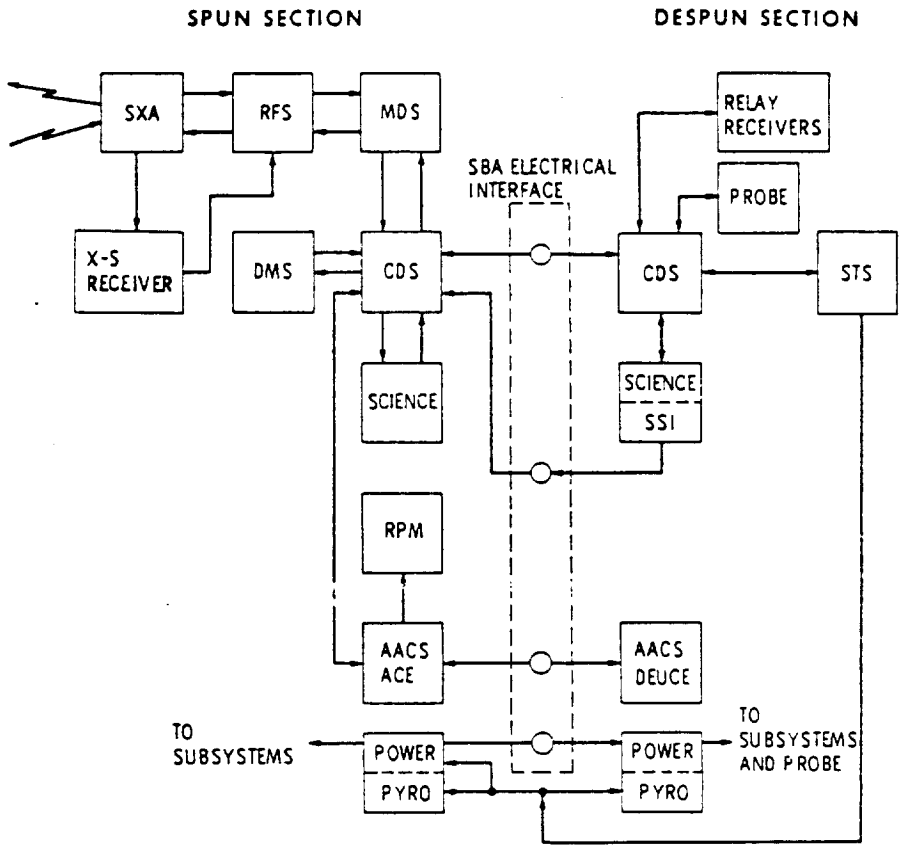


Figure 2.4-2. Simplified Spacecraft Block Diagram

2.4.2.3 Command and Data Subsystem (CDS) and Data Memory Subsystem (DMS). The CDS is an active, redundant microprocessor-based system with a total of 384K bytes of memory that utilizes data buses for interaction with other engineering subsystems, science instruments, and Probe relay receivers. Its functions are uplink command processing, programmed sequence storage and execution, fault protection, downlink data collection and formatting, and onboard intercommunications.

Ground commands are decoded by a hardware command decoder and responded to by sending the uplinked messages to the software elements of the CDS. Uplinked messages are assembled into a sequence of stored commands for later execution. In addition, CDS responds to spacecraft status indications from several spacecraft sensors. These measurements are placed in telemetry and also used to trigger fault responses. During the launch sequence, a stored program, activated by IUS discretes, controls the propulsion venting sequence, the boom deploy sequence, RF transmitter turn on, and thermal state.

The CDS also gathers and formats telemetry data for return to the ground for processing. Data are sent to the ground via X/S-band telemetry. The spacecraft tape recorder, the DMS, is utilized at several phases to record data for later playback.

2.4.2.4 Attitude and Articulation Control Subsystem (AACS). The AACS is also computer controlled and contains 64K, 16-bit words in Random Access Memory (RAM), and a 1K in Read Only Memory (ROM). The AACS points the spacecraft for Earth communications and Probe release, controls thrusters for attitude correction and maneuvers, points the scan platform, adjusts the RTG boom positions for wobble control, and controls the spacecraft spin rate and position of the despun section. The AACS receives commands and program updates from the ground via the CDS, as well as commands directly from CDS programs. Inputs from the gyros, accelerometers, star scanner, Sun acquisition sensor, spin bearing assembly, and scan actuator subsystem position encoders provide feedback required for closed-loop control.

Propulsion control consists of latching isovalves, drive signals to the 400-N main engine and the 12 10-N thrusters, and heaters on the two 10-N thruster clusters.

The subsystem operates in six different modes, including the launch and deployment modes, with mode selection by ground or CDS command.

2.4.2.5 Retro Propulsion Module (RPM). The RPM provides all of the propulsive maneuvers of the spacecraft after IUS separation. The RPM is a mechanical, separable self-contained module which is integrated as a load carrying part of the spacecraft spun section.

The RPM is a bipropellant pressure-fed system using the hypergolic propellant combinations of monomethyl hydrazine and a mixture of nitrogen tetroxide with a small fraction of nitric oxide added. Its four propellant tanks have a maximum usable capacity of 932 kilograms. The unified feed system supplies a central 400-N engine for the large maneuvers near Jupiter, and twelve 10-N thrusters for trajectory, attitude, and spin rate control.

2.4.2.6 Power/Pyro Subsystem (PPS). The PPS power electronic elements convert the RTG electrical output into regulated 30 V DC and 50 V AC spacecraft power. They distribute this power to all subsystems via latching relays controlled by the CDS.

The PPS pyro electronic elements consist of two pyro units (one spun and one despun) which store the energy necessary to fire all pyrotechnic devices. Each unit employs capacitor banks for energy storage and Silicon-Controlled Rectifiers (SCRs) for pyro initiation. Power to the pyro switching units and fire command are controlled by the CDS. Critical functions require two separate commands, one to enable the firing circuit and one to trigger the SCR.

2.4.2.7 Radioisotope Thermoelectric Generator (RTG). Galileo uses General Purpose Heat Source-Radioisotope Thermoelectric Generators (GPHS-RTGs) which represent a design evolution from those flown on the two Voyagers. The two RTGs convert heat from the radioisotope fuel (plutonium-238 dioxide) into electricity by silicon-germanium thermoelectric converters. The RTGs are located on articulating booms on the spun portion of the spacecraft. In addition, 130 single-watt Radioisotope Heater Units (RHUs) are used throughout the space- craft, and in several of the instruments.

There are two major components of an RTG, the GPHS-RTG and the converter, as well as support assemblies for the GPHS and a housing that encloses the generator and acts as a heat rejection radiator. The thermal energy provided to the converter comes from the GPHS, which consists of a stacked column of 18 individual modules, each providing about 245 watts from the decay of encapsulated plutonium-238 oxide which has a half-life of 87.8 years. The converter is composed of a thermopile that converts the radioisotope generated heat into electrical power. The thermopile consists of 572 silicon germanium (SiGe) thermoelectric elements called unicouples connected in a series parallel network.

2.4.2.8 Structure Subsystem. The structure subsystem mechanically supports all other spacecraft hardware. Its elements are designed with an ultimate factor of safety greater than or equal to 1.4 as required for STS safety. The structural loads and thermal environment used in the design of the spacecraft structure can handle worst-case launch and abort landing conditions.

2.4.2.9 Radio Relay Hardware (RRH) and Probe (PRB) Subsystems. The despun section of the spacecraft contains the radio relay hardware. This subsystem consists of redundant receivers, each of which relays Probe data to each of the redundant halves of the CDS. The Probe signal is received through the radio relay antenna which is articulated in cone to track the Probe during its travel in the Jovian atmosphere.

2.4.3 Fault-Tolerant Design Concepts

Several concepts are important to the understanding of the Galileo design. These concepts have to do with fault tolerance of the design and are described in the following sections.

2.4.3.1 Subsystem Redundancy. The spacecraft design incorporates redundancy at the subsystem level. In principle, each subsystem must allow for one failure without impairing the function of the spacecraft. For example, the CDS consists of redundant halves, each capable of commanding all spacecraft functions and collecting all critical telemetry. The AACS has redundant memories, processors, and input-output units which can be individually swapped. In some cases, full redundancy is impractical but can be achieved functionally. For example, the AACS inertial attitude system does not contain redundant gyros, but in the event of a failure, all control can be done using celestial sensors. In other cases, redundancy is impossible given spacecraft design constraints. There are two RTGs, for example, but the power from both is needed to achieve anything but minimal mission objectives. In subsystems such as this, the redundancy is built into the individual elements themselves. The GPHS of the RTG consists of many individual units, the failure of any one of which should not affect the others. The thermopile consists of a series parallel network of devices which cannot individually degrade a single RTG significantly. In summary, non-redundant subsystems are designed to have large demonstrated design margins.

In general, science subsystems are not redundant. Instead, the multiple science objectives of the mission insure significant return even in the event of the loss of one or two individual instruments.

2.4.3.2 Single Point Failure Policy. This design concept is best summarized in the Galileo single point failure policy, Project Policy 17:

No single failure of any electrical, mechanical, or electro-mechanical piece-part shall prevent:

1) Probe delivery.
2) Probe data acquisition.
3) Science data acquisition from more than one Probe instrument.
4) Successful Jupiter orbit insertion of the Orbiter.
5) Science data acquisition from more than one Orbiter instrument.
6) Acquisition of more than 50 percent of the Orbiter engineering data.

From this policy, it can be inferred that no single point failure that has not been placed on an exception list and analyzed in detail can cause an Earth avoidance concern.

This policy concept is expanded somewhat to preclude similar losses from two point failures which may be likely to occur in conjunction with each other, may be caused by the same event, are both more likely than the typical failure, or create a particularly mission catastrophic event.

Examples of such special cases of two point failures which have been protected against are:

1) No single failure in CDS combined with a single failure in the RRH shall prevent the return of Probe data.

2) No two failures in different CDS subelements shall prevent the operation of a functional CDS single string.

Furthermore, the likelihood of single failures has been examined and made consistent in the design. Some failures are extremely unlikely and not of concern. Others, however, approached a threshold of likelihood considered unsafe for the mission. When this happened, the failure mode was analyzed in detail and the design altered to eliminate the failure or reduce its likelihood to a safe level. This threshold of concern became apparent when a failure probability approached 1%. This made the probability of losing that system and its redundant component 10^{-4}, and amounted to an unacceptable mission risk. In general, 10^{-2} is considered an upper limit on the acceptable probability for any specific single failure. Similarly, 10^{-4} is an upper limit for any specific combination of two failures.

2.4.3.3 Fault Protection System. The Galileo spacecraft has been designed to be fault tolerant. This is accomplished not just through system redundancy and single point failure analysis, but through an extensive onboard fault protection system. Spacecraft hardware and software has been designed to respond to any spacecraft single fault by placing the spacecraft in a state in which it will be operable and safe for at least ten days. By that time, ground operators will be able to detect, analyze, and reconfigure the spacecraft for the remainder of the mission.

This fault protection system includes hardware elements such as the undervoltage detection and reconfiguration hardware. It also includes a significant amount of fault protection software: systems, CDS internal, and AACS internal. This software monitors a variety of detectable spacecraft faults and reconfigures the spacecraft in response to the most appropriate state for the current mission phase, including swapping in redundant subsystem elements. Specific fault protection programs include undervoltage recovery, command loss, RF loss, RPM overpressure, RPM thermal control, AACS heartbeat loss, science alarms, CDS loss, and a variety of AACS attitude and sensor failure responses. In addition, if either CDS or AACS undergoes a power-on-recovery (essentially a microprocessor reset), detailed software responses are selected appropriate to the failure type and the mission phase.

2.4.3.4 Failure Modes and Effects Analysis. For each subsystem, a failure modes and effects analysis was done as part of the critical design review. In this process, not only were the internal effects of failures on a subsystem analyzed, but so too were the effects on other subsystems, the overall system, and the mission. In each case, the analysis was evaluated using the single point failure policy and design inadequacies were eliminated.

SECTION 3

SPACECRAFT FAILURE MODE ANALYSIS

3.1 INTRODUCTION

A considerable analysis effort has been invested in the task of identifying all possible failures, both on the spacecraft as well as on the ground, that could cause an anomalous ΔV to be applied to the spacecraft, thereby changing its trajectory. This Section describes this effort in a summary form in order to provide an easily readable overview of the analysis that was performed and the results. A detailed and highly technical description of the work is included as an Appendix for the benefit of the reader with the background and interest to understand in depth how the specific results were obtained.

Failures which might incapacitate the spacecraft, but which would not cause any velocity perturbations, are not included in this effort because the navigation strategy summarized in Section 1 and described in detail in Section 4 insures that such failures cannot result in Earth impact. Likewise, failures occurring after the second Earth flyby are not included, since they also cannot lead to impact.

Most of the failures that can cause a ΔV to be applied to the spacecraft will not prevent the execution of a recovery maneuver if one is required to avoid impact. The probability of being able to implement such a recovery is dependent upon the nature of the failure and the time of occurrence of the failure relative to the time of the next Earth encounter. If the failure occurs well before the next encounter, and if it does not incapacitate the spacecraft, then the probability of recovey is very high. Conversely, if the failure occurs close to an encounter, there may not be adequate time to design and transmit the necessary commands. However, an ameliorating effect of these late failures is that a large ΔV is required to influence the trajectory enough to lead to an impacting trajectory. Hence, although the probability of recovery may be relatively low, the probability of needing such a recovery is also low. The recovery probabilities that have been used in this analysis are summarized in this Section, and a more detailed rationale for the values is given in the Appendix.

3.2 PROBABILITY OF SPACECRAFT FAILURES

Before proceeding with the description of failures and the analysis of each, the failure mode analysis will be put in perspective by presenting some general insights into the problem. This analysis is general in nature and does not strictly apply to every failure which will be later considered. It serves to give a sense of the reasoning that will be used in specific cases.

3.2.1 Probability of Single Failures

In general, every spacecraft subsystem was designed to be tolerant of single failures, either through redundancy, alternate operating modes, or otherwise. On a long duration mission such as Galileo, there is a significant probability that a failure will occur and the spacecraft must be tolerant of it such that the mission will not be lost. This strategy will be to no avail

if the likelihood of single failures becomes so high that it is likely that some subsystem and its backup will both be lost and the mission will fail.

In the design of each subsystem, special care was taken to minimize the likelihood of single failures. When the likelihood of a specific failure reached a certain threshold, the failure received significant attention. Through analysis or redesign, the probability of the failure was reduced below the threshold. The value of this threshold which required redesign was approximately 1% over the duration of the mission. In several specific cases in the Galileo design where failure-prone elements were discovered, specific Project policies were made requiring that the failure probability be reduced to less than 1% per subsystem over the life of the mission. Notable examples of this are the replacement of spacecraft memory components, both TCC-244 and HA6504RR11, and certain logic parts, RCA CD4049 and RCA CD4050. Hence, in general, the probability of failure of any specific subsystem on the spacecraft is less than 10^{-2}.

3.2.2 Probability of Double Failures

Single spacecraft failures can be tolerated through the activation of a redundant element with few exceptions. The exceptions have been specifically enumerated and exempted based on their low likelihood of occurrence. In general then, for a spacecraft disabling failure to occur, two failures must occur. They cannot be just two random failures, but one of a set of pairs of specific failures which, together, cause a spacecraft failure. The probability of any two specific failures is then the product of the probabilities of the individual failures or 10^{-4}.

3.2.3 Probability of Recovery

A detailed evaluation has been developed of the probability of the spacecraft being able to perform a maneuver to recover from an anomalous ΔV, given that the initial failure does not interfere with the recovery. This probability is then only a function of the time of the initial failure relative to the time of the next Earth flyby. There are several limiting factors, the importance of which depends on this time. The limiting factors are:

(1) A subsequent dual failure in the spacecraft which prevents further recovery operations.

(2) A subsequent single failure in the spacecraft which aborts the first recovery attempt, perhaps leaving insufficient time for further recovery attempts.

(3) An error made in the process of developing the recovery maneuver on the ground. By the time the error is discovered, there may be insufficient time to execute another recovery maneuver.

(4) The initial failure may occur so close to Earth flyby that there is insufficient time to plan and execute a normal recovery maneuver.

Table 3.1 presents a summary of these recovery failure categories, their relevant time domains, and the associated probability of no recovery. This Table will be used in later detailed failure probability evaluations. The Appendix presents the derivation of these numbers.

Table 3.1. Probability of No Recovery

Time of Failure Before EGA (days)	Probability of No Recovery
1. 20 or more	2×10^{-6}
2. 10 to 20	3×10^{-4}
3. 3-1/2 to 10	5×10^{-3}
4. 1 to 3-1/2	0.1
5. 8 hrs to 1	0.9

3.2.4 Failure Categories

The preceding discussion is useful for understanding the overall spacecraft design philosophy. It does not, however, apply to all failures, and several examples can be found where one or more of the assumptions do not hold. Specific problems have been found with micrometeoroid penetration failures which do not require two spacecraft failures, stuck thrusters where single point failures are possible, and the spacecraft drifting off its nominal Sunpoint where recovery may not be possible.

In order to better understand the spacecraft failure possibilities, a set of failure categories has been developed and each one analyzed to determine its probability and consequences. These results are summarized in the remainder of this section.

3.3 CATEGORIZATION OF FAILURES

All failures which can potentially cause a ΔV can be placed into one of three general categories. These categories cover failures that occur after the time of separation from the IUS and before the completion of the second Earth flyby. These categories also cover only those failures which may result in a ΔV. Failures which cause a loss of mission, but no possibility of Earth impact, such as those that occur after the second Earth flyby, are not included. The following are the three general categories of failures.

3.3.1 Spacecraft Failures

This category consists of all failures that occur due to internal failures in the spacecraft itself. It includes failures in any element of hardware or software that result in a failure of the subsystem to perform as designed. Such failures can be due to faulty parts, aging, hardware or software design errors not found in testing, or any other internal failure that causes the system not to meet its design requirements.

3.3.2 Environmental Failures

This category consists of failures which are externally induced. These failures result from the environments in space to which the spacecraft is subjected. Although the spacecraft has been designed to withstand such environmental effects, there is still some probability that the effect of micrometeoroid impacts or radiation, for example, may cause failures.

3.3.3 Ground Failures

The third category includes those failures which are induced in the process of controlling the spacecraft. It includes all failures induced through mission planning, operations, command generation, command transmission, and command reception by the spacecraft.

3.4 SPECIFIC FAILURES AND THEIR EFFECTS

This Section discusses specific failures and their effects, categorized within one of the general failures above. The specific failures identified and examined for spacecraft failures are propellant line or tank ruptures, stuck thrusters, thruster failures, electronic parts failures, structural failures, AACS software errors, CDS software errors, and spacecraft drifts off-Sun. The specific failures identified and examined for environmental failures are micrometeoroid penetration, radiation, and spacecraft charging. The specific failures identified and examined for ground failures are command generation and command transmission.

For each failure mode, the total probability of failure is given. These numbers represent the probability of a failure occurring between launch and the second Earth flyby which causes an anomalous ΔV. The derivation of these values, except for ones that are essentially zero, is contained in the Appendix. The probability that these failures will lead to Earth impact, considering the trajectory characteristics, the probability that the ΔV will cause an impacting trajectory, and the probability of being able to do a recovery maneuver, is developed in Section 4.

3.4.1 Spacecraft Failures

3.4.1.1 Propellant Line or Tank Failures. This category includes any hardware failure in the Retro Propulsion Module (RPM) which leads to escaping propellants or pressurant and results in an anomalous velocity imparted to the spacecraft. In analyzing the hardware failure modes of the RPM itself, it was discovered that by far the most likely failure mechanism was due to impact of RPM components by a micrometeoroid. No structural failure of propellant tanks or lines inherent in the hardware was determined to be as probable as the chance of tank penetration by a solid or liquified micrometeoroid. This failure category is analyzed in considerable detail in the Appendix as one of the environmentally induced failure categories. This failure mode is summarized below.

3.4.1.2 Stuck Thrusters. A stuck open or stuck closed thruster valve causes an anomalous velocity only during a maneuver (since only then are the isovalves opened). In this category the cause of the failure is a hardware failure in the thruster valve, the propulsion drive electronics (PDE), or the PDE annex. Other hardware and software failures which might cause anomalous thruster firing are covered in Sections 3.4.1.4, 3.4.1.6, and 3.4.1.7.

The specific failure mechanism here is that a component fails in the thruster valve or in the PDE, causing a thruster valve to stick, either open or shut, and an anomalous velocity results.

Figure 3-1 shows the orientation and nomenclature of the twelve 10 N thrusters. Note that each thruster designation indicates 'A' or 'B' plumbing branch, and thruster cluster number 1 or 2. Figure 3-2 shows a simplified schematic of the propellant tanks and plumbing. This Figure shows how the isovalves separate the 'A' and 'B' branch thrusters, and how isovalves and thruster valves must both be open before a thruster can fire. If only 'A' branch isovalves are opened, then no 'B' branch thruster can fire. Isovalves are opened only when a maneuver is about to begin, and are closed immediately upon completion.

The isovalves act as a safety net, limiting the damage that might be done by a stuck open thruster valve. An isovalve stuck open would not by itself result in imparted velocity. In any event, an isovalve stuck shut will result in no maneuver being performed. This analysis considered both isovalves and thruster valves stuck open, but the probability of such a double failure occurring was so small that it made a negligible contribution to the total probability.

When the spacecraft is close to the Sun (near Venus), a stuck open thruster could cause off-Sun attitude excursions which result in temperature damage to the high-gain antenna (HGA). Such damage could occur before baseline fault protection responded. As a result, the addition of the Sun gate and PDE annex devices were made to the spacecraft specifically to guard against a stuck open thruster failure.

The Sun gate is a photoelectric sensor which triggers an on-board fault protection response whenever the HGA-Sun angle exceeds a threshold due to some spacecraft malfunction.

The PDE annex detects and prevents an anomalous signal to a thruster valve when no signal was issued by the AACS I/O. Hence, the probability of the propulsion drive electronics (PDE) causing a stuck open thruster failure has been greatly reduced.

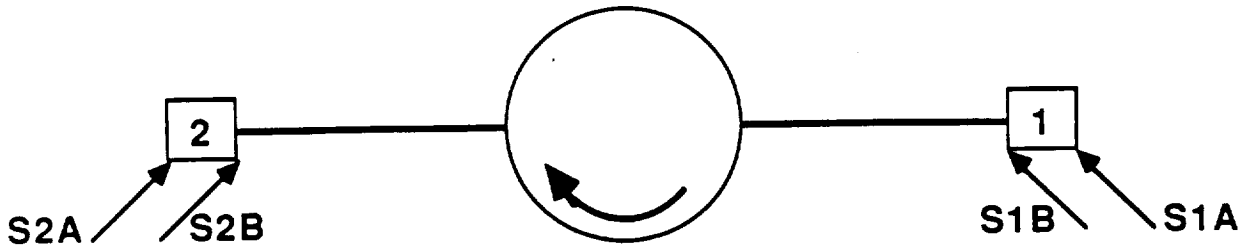
Since the data used in this analysis did not reflect the addition of the Sun gate or the PDE annex, the probability of stuck thruster failure will be substantially less than that used in this report.

Fault protection built into the spacecraft software will detect many stuck thruster failures. A failure in fault protection has not been included in this analysis because:

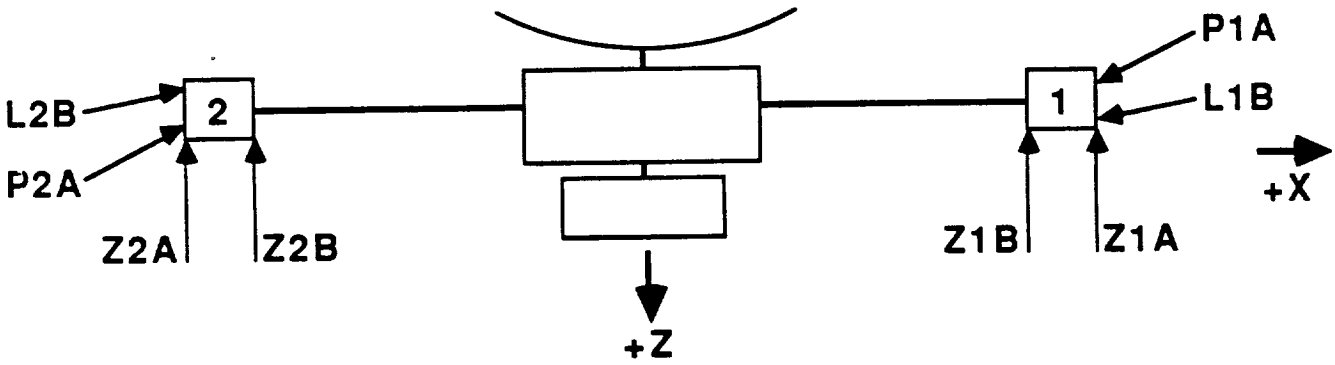
1) The probability of such a double failure occurring is extremely small, and

2) The values used for the probability of a stuck thruster are large since they do not reflect the addition of new failure protection devices (Sun gate and PDE annex).

Values for probability of recovery are obtained from Section 3.2.3. The stuck thruster failure does not preclude recovery since all propulsive maneuvers have an alternate thruster branch with independent plumbing.



SPACECRAFT TOP VIEW



SPACECRAFT SIDE VIEW

Figure 3-1. Thruster Nomenclature

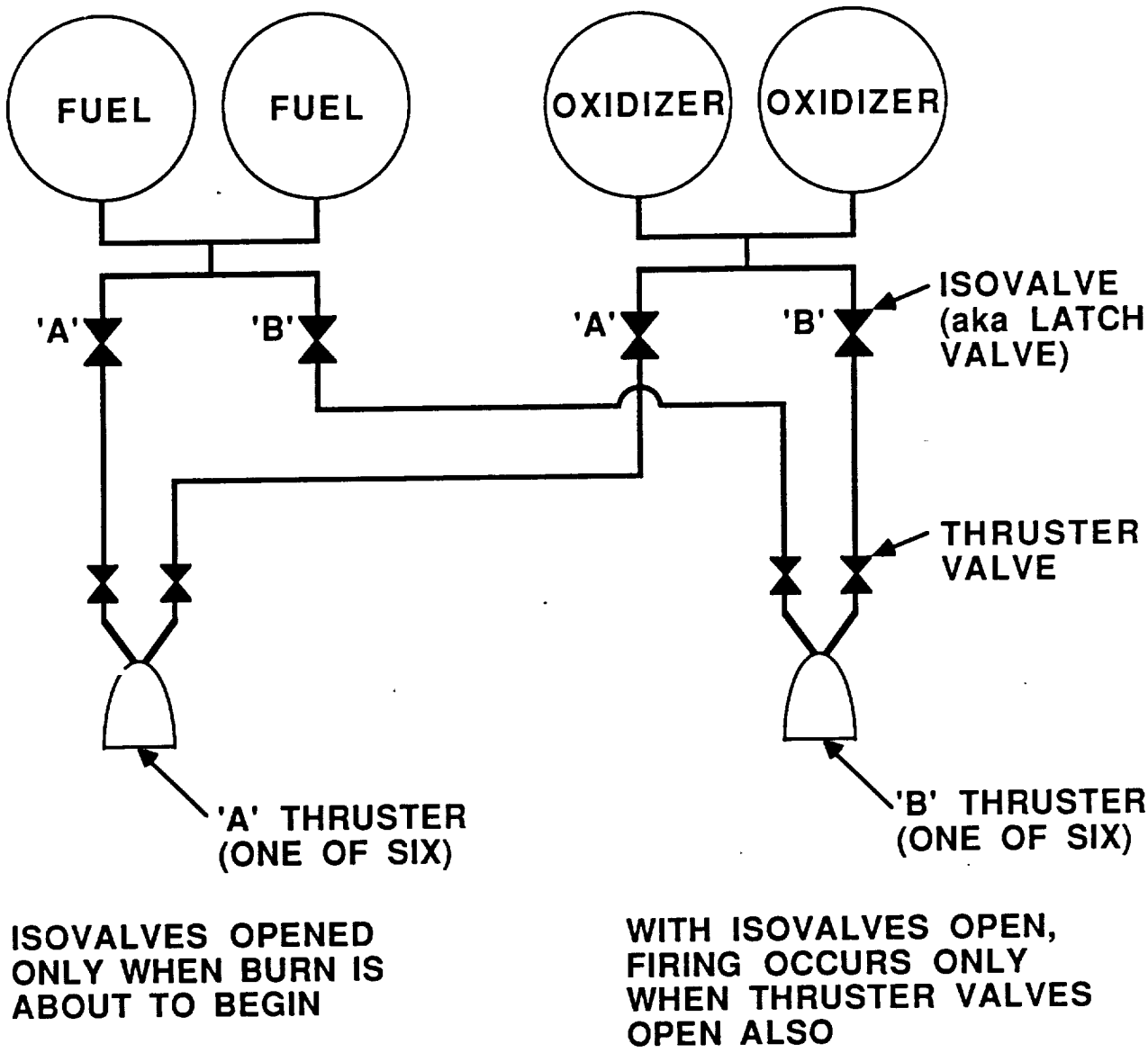


Figure 3-2. RPM Valve Nomenclature and Function

The total probability of a thruster sticking, either open or closed, sometime between launch and the second Earth flyby, has been determined to be bounded by 6.5%. The derivation of this result is given in the Appendix.

3.4.1.3 RPM Thruster Failure. A recent failure in another satellite thruster system which is based on the Galileo design has caused the Galileo Project to take a careful look at their thruster system. The satellite failed due to operating its thrusters at an operating point which caused thruster overheating and melting, as well as melting of the thermally coupled redundant thrusters. Since the Galileo spacecraft uses thrusters of similar design, but operating at a lower flow rate, an analysis was done to assure that similar failures were not a threat to Earth avoidance or the mission. The results of this analysis indicate that the thrusters are only at risk of failure when operated in the continuous mode, and then, based on fault protection currently being implemented, the worst-case outcome is an anomalous ΔV of 0.04 m/s. The spacecraft trajectory never can be made an impacting trajectory by a ΔV that small, no continuous burns are planned near Earth, and a recovery capability exists by using redundant thrusters in the pulsed mode. Consequently, this failure mode poses no risk to Earth avoidance.

3.4.1.4 Memory Failure. The worst-case failure in this category, in the sense that it is probably the most likely failure as well as having the most serious consequences, is where an AACS memory chip fails, causing an error in thruster firing control at the next TCM. The worst-case situation is a failed AACS memory chip that escapes detection until causing trouble during a TCM. Most AACS memory is checksummed (including all the code) and checksum region failures will be detected almost immediately, although the spacecraft takes no action other than setting an indicator in telemetry. Two failure classes are examined:

1) A failure that occurs outside of the checksum region such that there is no internal detection,

2) A failure that occurs in the checksum region within two days of a TCM such that there is insufficient time for detection and corrective action from the ground.

The analysis for these two cases, as developed in the Appendix, indicates the total probability of a memory failure causing an anomalous ΔV between launch and the second Earth encounter is 7×10^{-5}. The standard recovery probabilities are used, since a failure in one of the redundant halves of the AACS does not prevent normal use of the other half.

3.4.1.5 Structural Failures. Beyond the requirement to keep the spacecraft together, Galileo's structure plays a vital role in stabilizing the spacecraft. Galileo, like all spinning spacecraft, must have proper ballasting, structural alignments, and control of mass properties to remain dynamically stable. If, for example, an improperly designed piece of structure broke and released a large component, the resulting shift in mass properties would affect the spacecraft's rotation. At best, the spacecraft would be left with an uncorrectable wobble which would degrade telecommunications and science instrument pointing. At worst, the resulting nutation and wobble may make the spacecraft uncontrollable.

Given the navigation strategy which biases the spacecraft away from an impacting trajectory, even worst-case structural failures which release hardware will not lead to impact. The only hypothesized case where Earth impact could be imagined are failures where an RTG breaks free and flies off on its own trajectory. As will be shown in the following paragraphs, the spacecraft's design makes this scenario implausible.

By themselves, most structural failures produce little or no ΔV and so do not risk Earth impact. However, if an RTG could break free, its angular momentum would hurl it away from the remainder of the spacecraft. In addition to acquiring ΔV, the RTG would be uncontrollable and a potential hazard to the Earth.

This worst-case scenario is not credible for several reasons. First, all spacecraft structure, including the RTG booms, is designed with a large margin of safety (a factor of 1.4 or greater). Second, prior to launch, the entire spacecraft is exhaustively tested on a dynamic shake table to validate that all structural members can withstand launch vibration, the worst dynamic environment of the entire mission. Finally, even if an RTG boom could completely disintegrate, the RTG would still be retained by heavy electrical cables. These cables can easily hold the RTG even against the tension (about 40 pounds at 10 rpm) resulting from a stuck-open spin thruster (second failure) before onboard fault protection software intervenes. Although a dangling RTG would leave the spacecraft with a severe wobble, the RTG will remain with the spacecraft.

Given the design and testing practices which secure the RTG, there is no credible structural failure which could lead to an RTG becoming separated from the spacecraft. Accordingly, the probability of impact due to this failure type is treated as zero.

3.4.1.6 AACS Flight Software Coding Error. A flight software programming error might affect execution of some maneuver which fires thrusters. The software error could be present at launch, or it might be introduced by an in-flight software code change. A software error present at launch would almost certainly be detected by TCMs preceding the Venus flyby. It is more likely that such an error near an encounter would be introduced by an in-flight software change. No such in-flight software changes are planned until after the second encounter.

Only during a propulsive maneuver, when the isovalves have been opened, can a software error cause an anomalous thruster firing. HGA correction maneuvers will be performed approximately daily. Flight software code errors which affect the HGA correction maneuver would therefore be detected early. In spin correction maneuvers, an anomalous thruster firing would trip fault protection while imparting only a fraction of a meter per second at most. The worst situation is an error affecting vector mode maneuvers and not affecting HGA corrections. If an error caused a burn to be too big, the burn would be stopped by the backup command which is built into each burn sequence. However, an error in the burn control algorithm could cause a lateral burn to be executed in the wrong direction, anywhere in the plane perpendicular to the axial direction, or the selection of the wrong thruster, either of which would escape on-board detection.

Given the level of testing to which the software is subjected, it is estimated that the probability of discovering in-flight an AACS software coding error is bounded by 0.1 for the eight-year mission. In the Voyager mission to date, no such AACS software errors have been encountered during execution.

The probability density for error occurrence is taken to be uniform in time. An error in the critical section of code may or may not affect the burn results. If the error affects the burn magnitude only, it will not pose a risk to Earth avoidance because burns too large are stopped by the backup command, and burns too small cannot result in an impacting trajectory. If the error affects the burn arc or thruster selection, a burn of the right magnitude but in the wrong direction may result. A worst-case assumption is used, that the software error has a 50% chance of a resultant burn in the wrong direction. Backup commands will prevent imparting too much velocity, but the intended velocity magnitude may be delivered in the wrong direction. The velocity error may be lateral or axial with equal probability.

3.4.1.7 CDS Software Errors. The worst-case consequence of a software error in this category is one where the CDS sends an erroneous command to the AACS. To be accepted by the AACS, the command must have a correct checksum. In the worst case, the command causes the AACS to execute an anomalous burn.

The CDS is designed such that there is no more than a 1% chance of sending an anomalous command to the AACS during the mission. A 16-bit checksum is attached to every AACS command in order to prevent such anomalous commands from affecting the spacecraft. The most likely way for such a command to be received by AACS is for a valid command to be anomalously distorted into an AACS command which induces thruster action and for that command to have the checksum just happen to be correct. It should be noted that these probabilities only account for an erroneous command being sent by the CDS, and then being accepted by the AACS, with no allowance for the further reduction when considering the likelihood that such a command would lead to a thruster firing. This factor was not pursued in this analysis, since the probabilities are already so small. The probability of recovery from such a failure depends only upon the time available before encounter to recover. The initial failure does not interfere with recovery.

The total probability of a software error in either the AACS or CDS that causes a ΔV between launch and the second Earth encounter is 4.3×10^{-5}.

3.4.1.8. Thermal Failures. The Galileo spacecraft is protected from extreme temperature excursions by multi-layer insulation (MLI), which envelopes critical subsystems (including the four Retro Propulsion Module (RPM) propellant tanks), and by mechanical and structural shade devices. The thermal control systems are designed such that subsystem temperatures will remain within flight allowable limits as long as the angle made between the spacecraft's -Z-axis and the Sun remains less than 14°. If the spacecraft loses its sunpoint during the first three years of its mission, the resulting thermal problems could lead to failures which could cause a ΔV, either through inadvertent thruster firings or through an impulse due to RPM tank rupture.

Several thermally induced failures were examined, but only two were determined to be serious enough to analyze in detail. Electronic parts failures due to high temperatures resulting from off-Sun conditions are shown to have sufficiently low probabilities of causing ΔVs as to be of no concern. RPM tank rupture due to thermally induced overpressure was shown to be of significant concern; however, the Galileo Project has incorporated changes to the RPM design which will prevent the overpressure conditions that could lead to a rupture.

As the spacecraft moves through space, its pointing relative to the Sun must be continually corrected by the spacecraft attitude control system since the Sunpoint angle (the angle formed between the spacecraft's -Z-axis and the Sun) would otherwise change throughout the course of the trajectory around the Sun. The spacecraft would lose attitude control capability if both redundant halves of some element in the command chain failed. This could occur in the RFS, MDS, CDS, or AACS. A loss of commandability could cause the spacecraft to lose its pointing relative to the Sun. If either of these happened, then the spacecraft pointing relative to the Sun would begin to drift. The resulting off-Sun condition would eventually cause the RPM tanks to be directly exposed to solar heating and the tanks' high temperatures, without the design change mentioned above, would have caused an overpressure condition, resulting in a rupture and a resultant ΔV. Recovery possibilities would have been essentially non-existent due to the loss of propellant, even if the spacecraft's commandability were restored.

The off-Sun condition would also expose AACS PDE parts to excessive solar heating, causing them to overheat and fail. This parts failure could create an erroneous command, causing a large anomalous thrust with a resultant ΔV. There could be insufficient capability to recover the spacecraft from this failure.

It is noted that other electronics parts failures, such as memory failures, may lead to an anomalous thrust, but failure in the PDE leads to the most direct and most likely failure.

Other failures involving an off-Sun condition were considered, but are not worst case scenarios. For example, thruster valve failure due to drifting off-Sun is not probable because valves are acceptance tested to 115°C and are designed to survive to 160°C, but the valves' temperatures will always be less than or equal to the tanks' temperatures which will never exceed 114°C. Another example, stuck thrusters, is not a worst case cause of drifting off-Sun because although stuck thrusters are caused by a two point failure and they result in an unpredictable off-Sun condition followed by orbital drift, they tend to allow for recovery unlike the communication failure which assumes none.

The probability of this failure leading to a ΔV has been determined to be 1.5×10^{-6}.

3.4.2 Environmental Failures

3.4.2.1 Meteoroid Damage to Propellant Tanks. Although no interplanetary spacecraft is known to have suffered catastrophic meteoroid damage, meteoroid-induced failure of a propellant tank poses a potential hazard to the

Galileo spacecraft. The failure has the potential of expelling several hundred kilograms of propellant, imparting velocity to the spacecraft, and enveloping it in a cloud of caustic vapor. The resulting spacecraft damage makes a recovery maneuver unlikely.

Empirical knowledge of the solar system's meteoroid distribution is incomplete, especially for meteoroids large enough to harm propellant tanks. Extensive data exist for large meteoroids (based on lunar and Martian cratering) and for fine meteoric dust (estimated from zodiacal light observations), but little is available for intermediate sizes. Since the meteoroid sizes relevant to spacecraft failures include this intermediate range, this report must rely on available models which employ interpolations to predict the likelihood of tank failure. Where assumptions must be made, they have been chosen to err conservatively, overestimating rather than underestimating the risk. A detailed analysis was done of the interaction of micrometeoroids with fluid-filled tank walls and bumper shields, and how a micrometeoroid penetration affects a tank. The findings of all of these studies contributed to the results summarized here and described in detail in the Appendix.

Four spherical titanium tanks carry Galileo's 955 kg propellant supply. The fuel (monomethyl hydrazine) and oxidizer (nitrogen tetroxide) reside in tank pairs as shown in Figure 3-3. The innermost propellant tank halves are completely enclosed by solid spacecraft structure; thruster booms and electronic bays partially surround the outermost tank halves, but otherwise only their multi-layer insulation (MLI) lies between them and space.

The probability of a micrometeoroid-induced RPM tank failure causing a ΔV is 4.5×10^{-4}. Based on the questionable likelihood of being able to recover after such extensive damage, the probability of recovery is assumed to be zero. The manner in which the trajectory is designed to make the risk of impact as a result of this potential failure mode very small is described in Section 4.

3.4.2.2 Radiation. Although radiation has been carefully considered for its effects on mission reliability, it poses a negligible threat to Earth avoidance. This is due to the fact that the majority of the radiative effects that will be seen by the spacecraft occur in the vicinity of Jupiter. Galileo, like Voyager, is radiation hardened to the Jovian environment. The dose that it will receive by the time of the second Earth encounter is less than 5% of the total dose designed for in the entire mission. Earth avoidance protection from the two principal radiative effects, total dose and single event upsets, requires only a small fraction of the design margin required to withstand the Jovian environment. The probability of an anomalous ΔV resulting from these two effects is 1×10^{-4}. The standard recovery probabilities are applicable since this failure does not interfere with continued normal operation of the spacecraft.

3.4.2.3 Spacecraft Charging. Spacecraft charging also does not pose a significant threat to Earth avoidance. Both surface and internal charging have been considered. The most likely threat is from internal charging at the first Earth encounter which may affect the first maneuver after the encounter.

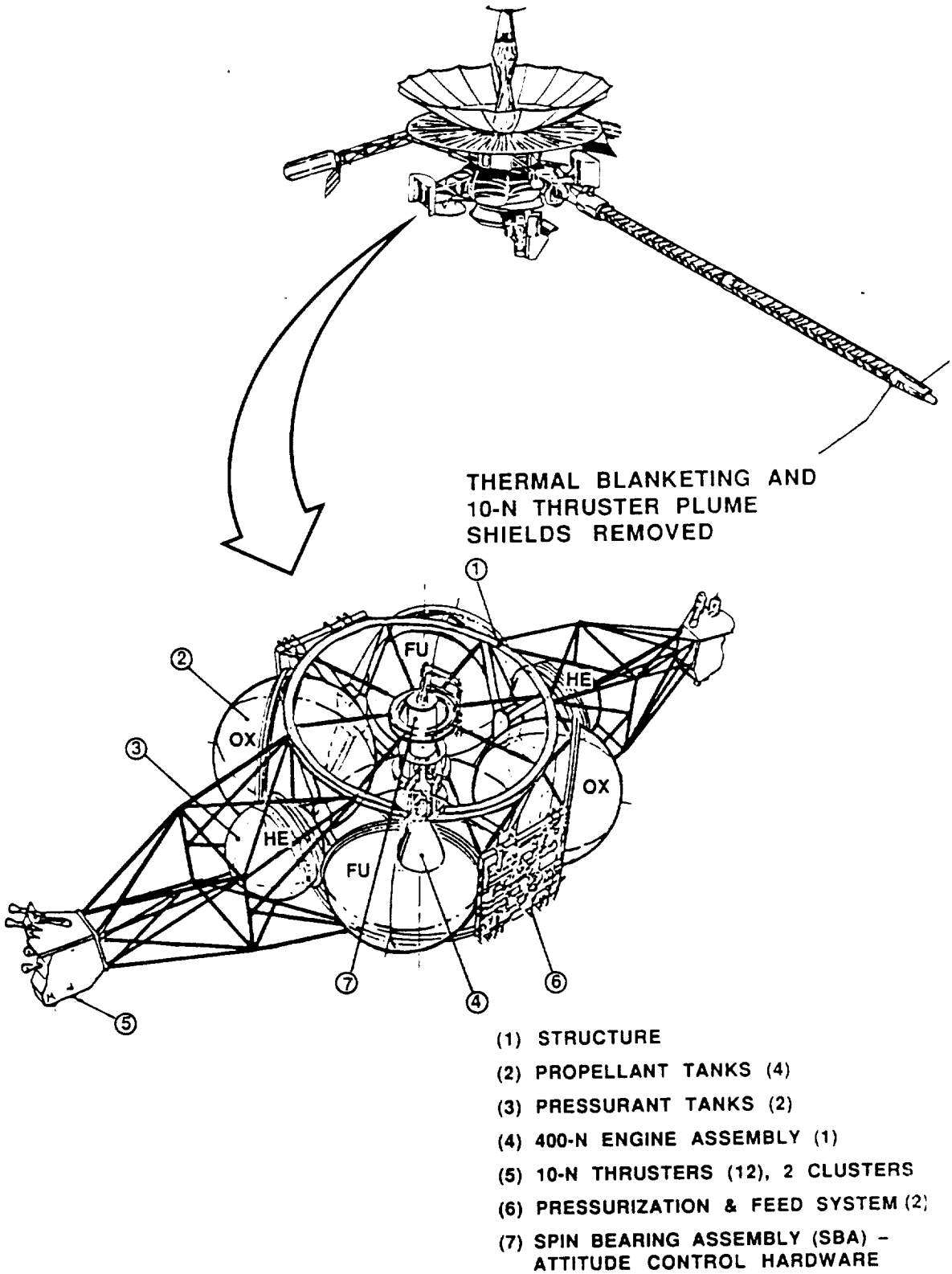


Figure 3-3. Propulsion System (RPM) Elements

Spacecraft charging is defined as the buildup of charged particles and subsequent arcing on external spacecraft surfaces or on (and inside) internal surfaces. The former process is usually referred to as surface charging while the latter is termed internal charging. Since each process is associated with a different charged particle population, the details of the charging processes are somewhat different. To accommodate this difference, the two processes and their associated probabilities are treated separately. Then, since the principle effect of the two, namely, induced electrical transients, is similar, the final probability for failure due to spacecraft charging is the sum of the two. Details of the development of this probability are given in the Appendix. The total probability of a ΔV resulting from spacecraft charging is 1.2×10^{-3}. The standard recovery probability values are applicable.

3.4.3 Ground Induced Errors

3.4.3.1 Command Generation. The sequencing process for generating and checking commands for the spacecraft is described in Section 2.3. This section will describe the most probable scenarios for errors to occur in that process. Command generation errors occur due to the combined failures of automated software checks and procedural checks (human error).

There are four ways to get an erroneous maneuver command to the spacecraft:

1) Send an erroneous individual maneuver command, instead of another command, or instead of no command.

2) Send an erroneous value in any maneuver Profile Activity (PA).

3) Send an erroneous maneuver PA instead of another PA, or instead of no PA.

4) Send an accurately built maneuver PA that reflects the Navigation Team's requested maneuver, but the Navigation Team has internally made an error.

In generating these scenarios, only the case where one erroneous command is sent, or one erroneous PA is sent is considered. Cases with multiple errors are considered even less probable. The exception to this is where Navigation erroneously requests an incorrect maneuver. To cover worst case situations, each error is assumed to be introduced as late as is possible in the Uplink Sequence Generation process. The sequence checks are derived from Galileo Space Flight Operations Plan (625-505, Vol. II, Operating Plans).

3.4.3.2 Uplink Transmission Errors. The failure mode considered here is where a correctly generated sequence is corrupted during the process of transmitting it to the spacecraft, and then the spacecraft accepts it as a valid sequence and initiates thruster firings.

The details of the sequence generation and uplink failure analyses are contained in the Appendix. The total probability of these failure modes leading to an erroneous ΔV are derived to be 5×10^{-3}.

Table 3.2. Spacecraft Failure Probability Summary

Failure Mode	Probability of Failure Occurring and Causing a ΔV
Propellant Line or Tank Failure	0
Stuck Thrusters	0.065
Thruster Failure	0
Memory Failure	7×10^{-5}
Structural Failure	0
Flight Software Error	4.3×10^{-5}
Thermal Failure	1.5×10^{-6}
Micrometeoroid-Induced Failure	4.5×10^{-4}
Radiation-Induced Failure	1×10^{-4}
Charging-Induced Failure	1.2×10^{-3}
Command Generation and Transmission Failure	5×10^{-3}

SECTION 4

NAVIGATION PLAN

4.1 INTRODUCTION

This Section presents the navigation strategy for designing and implementing the trajectory between launch and the second Earth flyby. The goal of the navigation strategy is to develop a method for selecting a sequence of target parameters for each maneuver such that the mission is successfully targeted to Jupiter while the probability of an inadvertent reentry into the Earth's atmosphere is made very small and propellant cost is kept within reasonable bounds. The method will necessarily be adaptive to changing conditions as the mission is flown. The goal here is to specify a set of design criteria and rules which will determine the design and flight profile of the Galileo mission. This strategy takes into account all of the failures covered in Section 3, as well as other types of failures which could disable the spacecraft without producing a velocity change. Finally, this Section also provides an upper bound on the probability of Earth impact as a result of this strategy.

As it turns out, there are only two failure types which tend to dominate the design process because of their higher (relative) probability of occurrence. That is, if the trajectory is modified to safely accommodate failures from these categories, the other conceivable failure scenarios will be at least one and, in some cases, several orders of magnitude less significant. If these failures are accounted for, it will be shown that the other failures will be covered as well.

Section 4 is divided into three parts. The first part (Sections 4.2 through 4.4) presents the general criteria and techniques that have been used to design a trajectory which will satisfy Earth avoidance concerns. The second portion (Section 4.5) is a detailed look at the application of these methods to each maneuver between launch and the second Earth flyby for a sample trajectory. Finally, the last part (Section 4.6) contains a summary of the impact probabilities and an examination of the sensitivities of these calculations to certain modeling assumptions.

4.2 FAILURE INFLUENCES ON THE TRAJECTORY

To understand the reasons for the various choices made, it is necessary to categorize the failures and the possible responses that the Galileo spacecraft system can make in the presence of failures.

At the highest level, there are two types of failure modes that can result in a trajectory which leads to Earth impact. Each potential failure in the Galileo spacecraft can be separated into one of these two categories, based upon whether or not the failure alters the trajectory; that is, is the failure capable of generating a velocity change (ΔV)?

The first is a failure which affects the performance of the spacecraft, while not altering the trajectory. An example of such a failure might be a loss of uplink capability which results in the inability to command the spacecraft. It is theoretically possible, although very unlikely, that

prior to the failure, the spacecraft could be on an impacting trajectory due to the dispersions which arise from launch injection errors, maneuver execution errors, or orbit determination errors. Normally, if the spacecraft were on an impacting trajectory as the result of these dispersions, corrective actions would be taken immediately. However, if such a failure were to occur, the performance of a corrective maneuver could be precluded. For purposes of discussion below, any failure which does not cause a ΔV will be designated as Type I.

The second mode is one in which the spacecraft is on a nominal non-impacting trajecory and a system failure occurs which imparts an unexpected ΔV to the spacecraft. The ΔV vector could be of sufficient magnitude and in the necessary direction to cause an Earth impacting trajectory. One such failure might be the unforeseen opening or closing of a thruster valve during a maneuver. Another possibility is the rupturing of a fuel tank with a ΔV imparted by the escaping propellant and/or pressurant. Such a failure will be referred to as a Type II failure below. Section 3 has provided a detailed analysis of Type II failures.

A failure which can cause an Earth impacting trajectory can be further classified according to whether or not recovery is possible. If the failure does not completely incapacitate the spacecraft, then it may be possible to command a recovery sequence to correct the trajectory and avoid Earth reentry. Associated with the probabilistic analysis of failures is an analysis of the probability of recovery, which is factored into the final impact probabilities.

For the purposes of aimpoint design and impact probability calculations, each of the failure modes in Section 3 must be further categorized as to whether the spurious velocity occurs during a maneuver, that is at a discrete point during the trajectory, or during cruise, where the probability of occurrence must be integrated over the period of vulnerability to the failure. Table 4-1 lists each of the failures analyzed in Section 3, the appropriate trajectory regime (cruise and/or maneuver) where each applies, and the relative probability of recovery. As will be seen later (Section 4.4), the events which have a low probability of recovery will generally dominate the impact probability calculations.

Table 4-1. Failures Which Can Cause a ΔV

Paragraph	Description	Type	P(Recovery)
3.4.1.1	RPM Tank Failure	Cruise	Low
3.4.1.2	Stuck Thruster (Maneuver)	Maneuver	High
3.4.1.2	Stuck Thruster (HGA correction)	Cruise	High
3.4.1.2	Stuck Thruster (Spin correction)	Cruise	High
3.4.1.3	RPM Thruster Failure	Maneuver	High
3.4.1.4	AACS Memory Chip Failure	Maneuver	High
3.4.1.5	Structural Failure	Cruise	Low
3.4.1.6	AACS Programming Error	Maneuver	High
3.4.1.7	CDS Software Failure	Mnvr./Cruise	High

Table 4-1. Failures Which Can Cause a ΔV (contd)

Paragraph	Description	Type	P(Recovery)
3.4.1.8	Off-Sun Thermal Failure	Cruise	Low
3.4.2.1	Micrometeoroid Impact	Cruise	Low
3.4.2.2	Radiation-SEU Effect	Maneuver	High
3.4.2.3	Spacecraft Charging	Maneuver	High
3.4.3.1	Command Generation Process	Mnvr./Cruise	High
3.4.3.2	Uplink Command Errors	Cruise	High

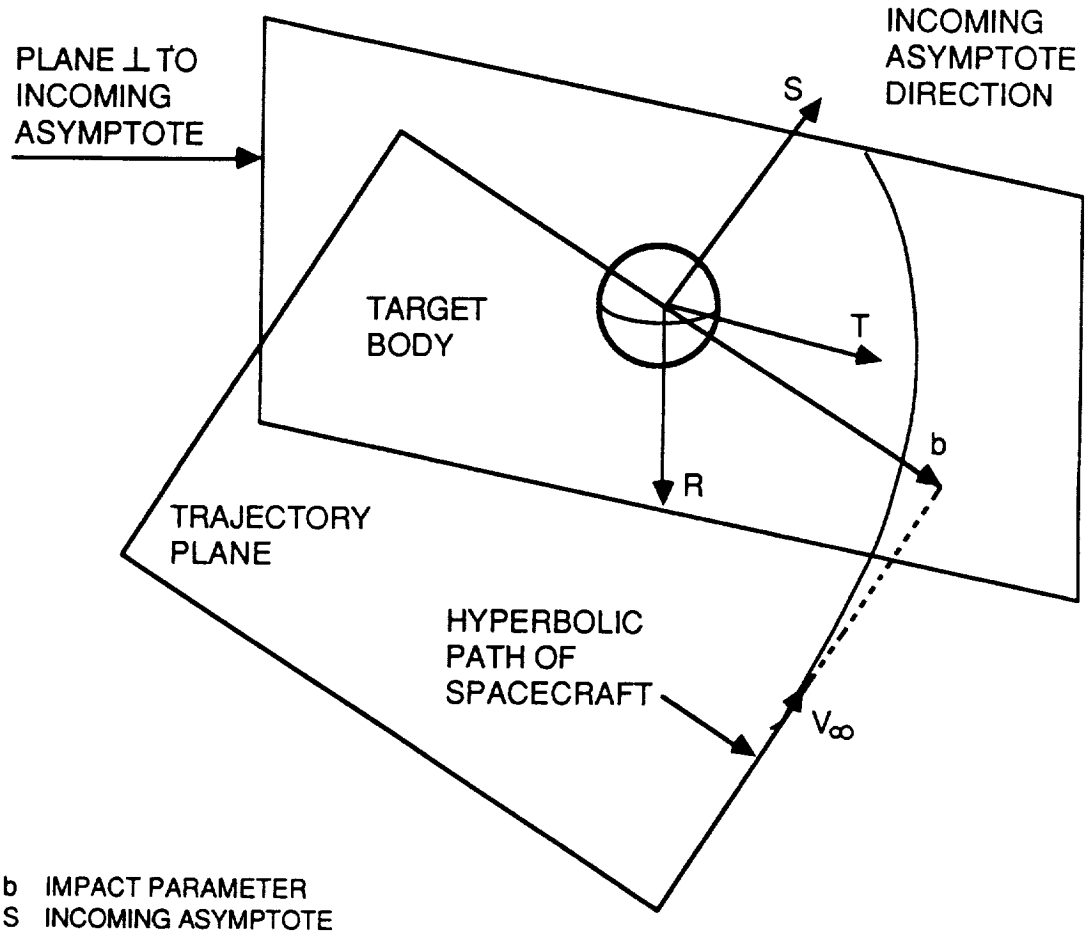
4.3 EARTH IMPACT AND PROBABILITIES

The trajectories from launch to Jupiter are developed using highly accurate double precision numerical integration with an N-body model of the solar system, as well as detailed models for solar pressure and the gravitational fields of the planets. For perturbations of these trajectories by velocities resulting from the types of failures listed above, two body conic elements are used to describe the encounter conditions and linear perturbation techniques with K-matrices used to relate changes in the encounter conditions to position and velocity along the trajectory. The K-matrices are generated using a fully integrated trajectory with the same models used to generate the design trajectories.

The osculating hyperbolic orbit at the time of closest approach to the target body defines a coordinate system known as the B-plane (Figure 4-1). The point where the extended V_∞ vector intersects this plane is known as the impact parameter or b-vector. All of the flyby targets' encounter parameters will be expressed in this coordinate system. Typically the b-vector is written as an ordered pair of its projections onto the R and T axes; b = (b•R, b•T).

Associated with any hyperbolic flyby, there is a minimum distance in the B-plane known as the impact radius (Figure 4-2), such that if the impact parameter lies within that distance, impact with the target body will occur. This radius, B_{IR} given by Equation (4-1), depends only upon the planet's gravitational constant μ, radius r_0, and the V_∞ of the trajectory.

$$B_{IR} = r_0\left[\frac{2\mu}{r_0 v_\infty^2} + 1\right]^{1/2} \qquad (4\text{-}1)$$



b IMPACT PARAMETER
S INCOMING ASYMPTOTE
T PARALLEL TO EARTH ORBITAL PLANE AND NORMAL TO S
R S X T

Figure 4-1. The B-Plane

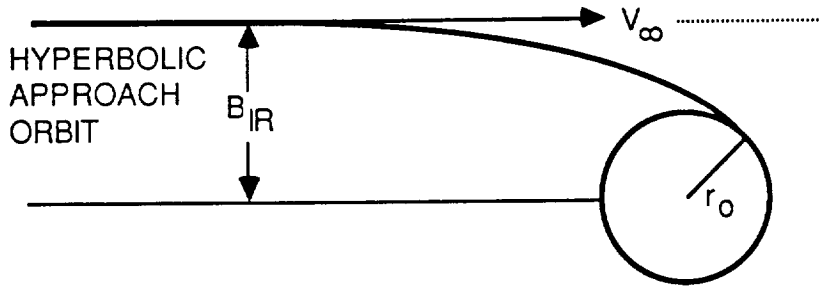


Figure 4-2. Impact Radius B_{IR}

For the purposes of this report, an extra 100 km has been added onto the Earth's radius as a conservative upper limit of the extent of the Earth's atmosphere where capture could occur. Thus, an Earth impacting trajectory is defined as any trajectory which has a radius of closest approach less than 6478 (6378 + 100) km. Effects which would tend to lower this limit, such as density models of the atmosphere and atmospheric skipping, have not been modeled. Without these factors included, the model is more conservative and simpler. Table 4-2 lists the impact radii and other parameters for the Earth flybys for an October 9, 1989 launch date. For this launch date, the flyby altitudes for EGA1 and EGA2 are as low as they will be during the entire 1989 launch period.

Table 4-2. Earth Flyby Parameters

	Earth 1	Earth 2
Altitude	970 km	303 km
V_∞	8.99 km/s	8.88 km/s
b	11248 km	10593 km
B_{IR}	10290 km	10367 km

4.3.1 Calculation of Type I Impact Probabilities

During the course of the mission, the exact conditions of the currently targeted flyby conditions at the Earth encounters will not be precisely known. This is the inevitable result of uncertainties in the orbit determination process, as well as variations in the performance of the propulsion system. At any particular point in the mission, say after the completion of a maneuver, the uncertainty in the the Earth encounter

conditions are modeled by a Gaussian distribution and can be graphically represented in the B-plane by a target (mean) and a dispersion (covariance) ellipse (Figure 4-3). Let b_0 denote the mean target and let Σ denote the covariance matrix. As indicated in Figure 4-3, the only dispersed points which result in an impacting trajectory are those which intersect the impact circle, a circle of radius B_{IR} centered at the origin. Thus, conditional upon there being no further corrective maneuvers, the probability of being on an impacting trajectory, p_i, given this mean aimpoint and dispersion, is just the integral of the Gaussian density over the impact circle [Equation (4-2)]. Numerical techniques have been developed to accurately evaluate these values.

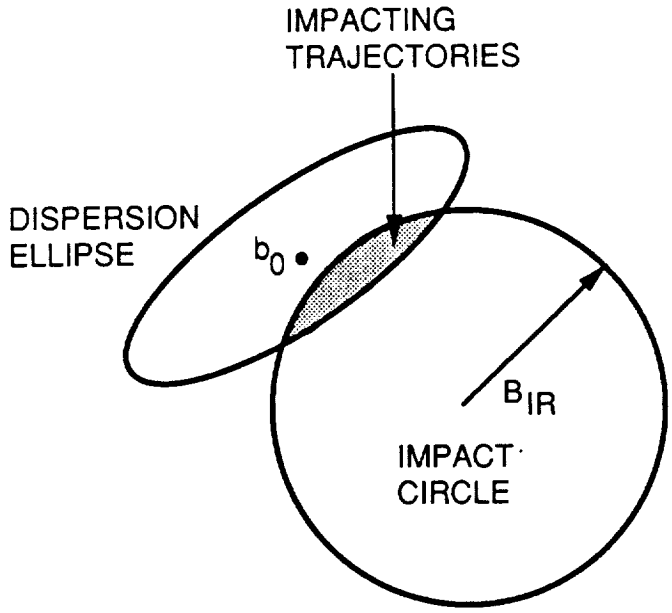


Figure 4-3. B-Plane Projections of Target, Impact Circle, and Sample Dispersion Ellipse

$$p_i = \frac{1}{2\pi|\Sigma|^{1/2}} \iint_{|b| \leq B_{IR}} \exp\left(\frac{-1}{2}(b-b_0)^T \Sigma^{-1}(b-b_0)\right) db \qquad (4\text{-}2)$$

Suppose that the probability for a failure which precludes further maneuvers occurring during a particular time period (say until the next maneuver) is p_f and that the probability of recovering from this failure is p_r. Then, the total impact probability for this failure, assuming that there are no maneuvers in this period, will be

$$P(\text{Impact}) = p_i p_f (1 - p_r) \qquad (4\text{-}3)$$

where p_i is given in Equation (4-2). Equation (4-3) indicates that the probability of Earth impact from a Type I failure is simply the probability of being originally being on a impacting trajectory (Equation 4-2) times the probability of a failure occurring which would not allow a maneuver to correct the trajectory.

4.3.2 Calculation of Type II Impact Probabilities

For each failure category in Section 3, the analysts have provided a probability of that failure occurring, as well as the density function for the possible ΔV which could arise from that failure. Suppose that the current target of the spacecraft is b and that a spurious velocity v has occurred. Then, an impacting trajectory will result if and only if

$$\|b + Kv\| < B_{IR}$$

where K is the 2x3 K-matrix mapping velocity into the B-plane for the epoch of the impulsive velocity v (Figure 4-4).

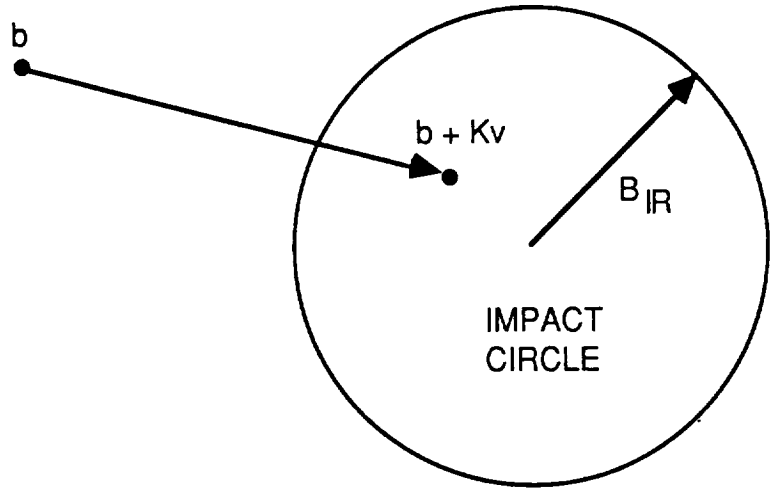


Figure 4-4. A Velocity Error v, Which Causes an Impacting Trajectory

If the spurious velocities are distributed according to the probability density function $\varphi(v)$, which is nonzero only on a region S in velocity space, then the probability of impact given that the velocity has occurred and that the spacecraft is currently targeted to b is given by

$$\tilde{p}_i(b) = \int_S \chi\,(b+Kv)\varphi(v)dv \qquad (4\text{-}4)$$

where

$$\chi(b+Kv) = \begin{cases} 1 \text{ if } \|b+Kv\| < B_{IR} \\ 0 \text{ otherwise.} \end{cases}$$

Taking into account the fact that the current target b of the spacecraft is itself a statistical quantity with mean b_0 and covariance Σ gives the total probability of impact given that the specified failure has occurred.

$$p_i = \frac{1}{2\pi|\Sigma|^{1/2}} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \tilde{p}_i(b)\exp\left(-\frac{1}{2}(b-b_0)^T\Sigma^{-1}(b-b_0)\right)db \qquad (4\text{-}5)$$

If the probability of a particular failure occurring, again denoted by p_f, and the recovery probability p_r are factored in, the probability of impact from this failure is also expressed by Equation (4-3). In this case, the probability of Earth impact from a Type II failure is simply the probability of the failure resulting in an impacting trajectory (Equation (4-5)) times the probability of a failure occurring which would not allow a maneuver to correct the trajectory. Note that, depending on the complexity of the evaluation of φ, the evaluation of Equation (4-5) can be a five-dimensional integral (three components of velocity and two components in the B-plane). Techniques for accurate evaluation of Equation (4-5) have been developed.

4.4 PROTECTING AGAINST SPACECRAFT FAILURES

There are two distinct ways that failures can be accommodated so that the probability of Earth impact is reduced to an acceptable level. The first is to modify the spacecraft components which have been identified as most likely to contribute to a failure resulting in an Earth impacting trajectory. For example, the spacecraft propellant tanks have been fitted with pressure relief valves which will dissipate the propellant in a controlled fashion should the tanks overheat. This modification makes the probability of this failure causing Earth impact effectively zero. In some cases, it is not possible or practical to modify the spacecraft. The only remaining option is to modify the trajectory.

A simple technique for modifying the trajectory would be to raise the altitude of the Earth flybys. The idea is that presumably there is an inverse relationship between the altitude of the Earth flyby and the probability of reentry. By increasing the altitude sufficiently, reentry should become more and more unlikely. Unfortunately, the relationship between flyby altitude and probability of reentry is fairly weak in light of the spacecraft failures which are most likely to cause reentry. Thus, it would be necessary to shift the altitudes of the Earth flybys by several thousand kilometers. With these alterations, the mission would not be possible. The spacecraft cannot carry enough propellant to make up for the energy shortfall from raising the Earth flyby altitudes.

Another technique is to design the trajectory as optimally as possible within the given constraints on minimum flyby altitude, then modify the way it is flown. This process has been used in past JPL interplanetary missions for planetary protection stemming from biological contamination concerns. The idea is that rather than aim directly at the final target altitude for each Earth flyby, the spacecraft will sequentially move into the final altitude at discrete time periods in the mission. The final target parameters as specified in the design will be achieved but in sequential

fashion. The increments in target altitude and time will be determined in such a way that if there is a spacecraft failure during a particular time period, the probability of this failure causing reentry will be minimized and in many cases eliminated altogether. This will achieve the goal of making the impact probability very small in a propellant-efficient manner.

4.4.1 Ground Rules

In the design approach for Earth avoidance, it has been productive to impose several overall restrictions upon the aimpoint selections and maneuver strategies, the first of which is:

1) At no point during the mission between injection and EGA2 will the probability of being on an Earth impacting trajectory following the successful completion of a maneuver be greater than 10^{-6}.

The figure of 10^{-6} was selected as a value that was feasible to achieve in terms of additional propellant consumption, and at the same time small enough to eliminate all concern for Type I failures.

Needless to say, if the spacecraft were to end up on an impacting trajectory due to navigation dispersions associated with the successful completion of a maneuver, the Navigation and Orbiter Engineering teams would design and implement a corrective maneuver as quickly as was operationally feasible and safe.

As indicated below, this rule will need to be applied in the few instances where navigation dispersions are relatively high, such as when low dispersions at a previous flyby are amplified by the flyby or there is a large maneuver with correspondingly larger dispersions. What this rule (together with Rule 2 below) accomplishes is to remove all concern about any Type I failure. Because of the spacecraft's high fault tolerance and a conservative estimate of the probability of failure to recover of at most 5×10^{-3} over the time interval where maneuvers are performed from Section 3.2.4, this guarantees an impact probability from Type I failures of less than 5×10^{-9}.

2) If, during the course of performing a maneuver, the maneuver were to inadvertently terminate, the probability of an Earth impacting trajectory resulting will no greater than 10^{-6}.

Rule 2 is an adjunct to the first rule in the sense that it requires that not only are the final target parameters for each maneuver constrained by the 10^{-6} level, but also the path which the maneuver traces from initial to final aimpoint in the B-plane. Notice that in particular rule 2 implies that at no point during the course of a maneuver will the path from the initial point to the desired target cross the impact circle. This insures that if a maneuver fails to complete, there will be no possibility of an Earth impacting trajectory.

3) The minimum perigee altitude that the spacecraft shall be targeted to prior to 25 days before an Earth encounter shall be 3000 km for EGA1 and 2000 km for EGA2.

Rule 3 is a protection from Type II failures. By targeting to the higher altitudes until the final 25 days, a larger spurious velocity increment must be realized in order to cause an impacting trajectory. In particular, if there is an unexpected overburn during a maneuver, there is much less probability of this resulting in an impacting trajectory when targeted to the higher altitudes. During the final 25 days, when Galileo will be targeted to the final target altitude, a larger spurious velocity would be necessary to cause an impacting trajectory anyway. This is due to the fact that the velocity required to cause an impacting trajectory is inversely proportional to the time from encounter. The difference in the rule for the two flybys accounts for the fact that the spacecraft system integrity and performance will be better understood by EGA2 as well as accommodating the lower EGA2 target altitude.

4.4.2 Failure Categories and Their Influence on Aimpoint Selection

Following is a list of the failure types and their effect upon the aimpoint selection process. As shown below, there are really only three types that have directly affected the process. These are navigation dispersions, stuck thrusters, and micrometeoroid impact. Once these failures have been accommodated by the aimpoint selection process, the other failures are also covered.

4.4.2.1 Navigation Dispersions. Type I failures are accommodated by the first ground rule. The first ground rule is a strict requirement on several of the maneuver aimpoints, as well as the flyby conditions for Venus, EGA1, and the asteroid encounter between EGA1 and EGA2. The situation for the Venus flyby is illustrated in Figures 4-5 and 4-6.

In some cases, the optimal trajectory between Venus and EGA1 is ballistic (i.e., there is no substantial trajectory altering maneuver between the two encounters). If the trajectory were ballistic between Venus and Earth 1, then nominal delivery at Venus would result in a mean impact parameter at Earth 1 of at most a few thousand kilometers away from the impact circle. If the dispersions about Venus are mapped to Earth and centered around this point, as in Figure 4-5, the probability of an impacting trajectory resulting is 2×10^{-2}. This is unacceptably high and precludes the use of a ballistic trajectory. The post-Venus aimpoint must be coerced outside of a region around Earth 1. Figure 4-6 illustrates the region this constraint implies. The elliptically shaped region represents a 1×10^{-6} equiprobability contour. If the post-Venus aimpoint lies inside the region, then, with the navigational dispersions at Venus, there can be an Earth impacting trajectory with a probability greater than 1×10^{-6}. By the first ground rule, the post-Venus aimpoint is to be outside this region. Given this constraint, the optimal aimpoint placement is as indicated.

Exactly the same criterion must be applied to the first Earth flyby and to the asteroid flyby. Given nominal delivery to the encounter, the probability of an Earth impacting trajectory must be less than 1×10^{-6}.

4.4.2.2 RPM Tank Failure. As indicated in Section 3.4.1.1, this is not considered a credible failure mode unless there are environmental effects and is covered below under micrometeoroids and thermal failures.

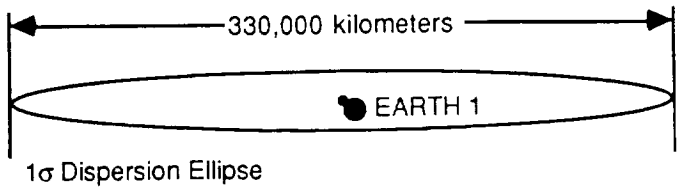


Figure 4-5. Post-Venus Dispersions About Optimal Earth 1 Target

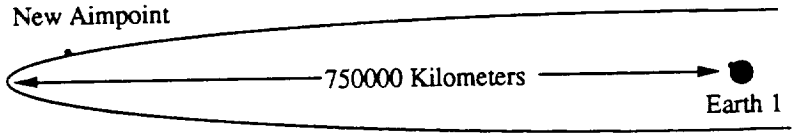


Figure 4-6. Equiprobability Contour of 1×10^{-6}

4.4.2.3 Stuck Thrusters. A stuck thruster on the Galileo spacecraft can cause a ΔV to occur in either the wrong direction or with the wrong magnitude. Wherever possible, the targets have been designed so that a maneuver of less than or equal to the correct magnitude and in any direction will never lead to an impacting trajectory. Referring to Figure 4-7, the maneuver is designed to go from b_0 to b_1. The achievable aimpoints from b_0 by a maneuver of less than or equal to the correct magnitude and in any direction are indicated by the ellipse. As indicated, the impact circle cannot be reached by such an erroneous maneuver.

In the case of too large a ΔV, a majority of these cases will be covered by ground rule 3, which protects from an overburn. Thus, a large percentage of the possible thruster faults can be eliminated as causing any risk of impact by the design.

An additional aspect of some of the thruster faults is that they cause a ΔV in a very particular direction. For instance, a stuck thruster during a spin correction or HGA correction can only cause a small ΔV along the spacecraft's Z-axis. For a large portion of the trajectory, the ΔV is neither large enough nor in the right direction to ever cause an impacting trajectory.

Of those remaining failures which can cause an Earth impacting trajectory, there is a very high probability of recovery which makes these failures of secondary concern.

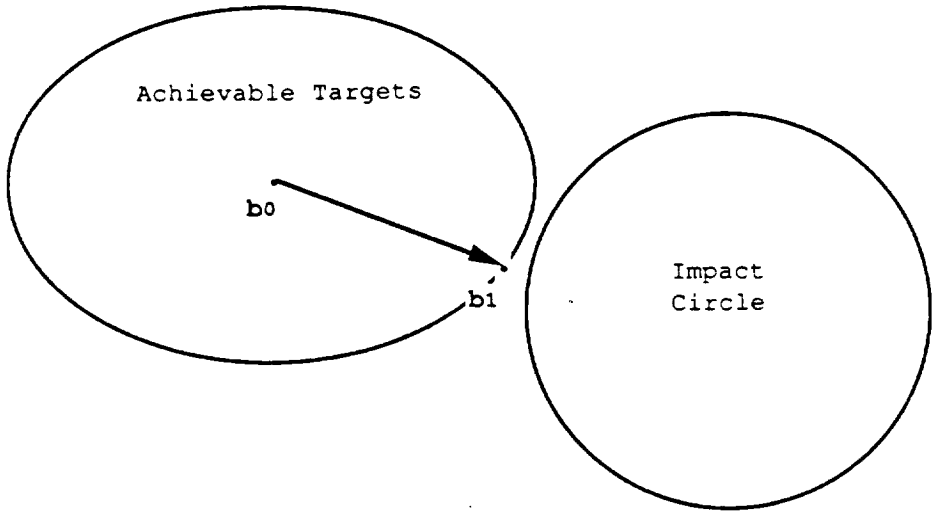


Figure 4-7. Achievable Targets From a Maneuver Which Burns Short in Any Direction

4.4.2.4 RPM Thruster Failure. A thermally induced failure of an RPM thruster can cause at most 0.04 m/s of ΔV. Given the biasing strategy chosen to follow the ground rules, this amount can never cause an impacting trajectory. Thus no special measures need be taken for this failure mode.

4.4.2.5 AACS Memory Chip Failure. The result of an AACS chip failure is analogous to the stuck thrusters mentioned above in that the result is a ΔV from a maneuver that was not in the expected direction and/or of the correct magnitude. The same measures that were taken to account for stuck thrusters also apply to the AACS memory chip failure scenario. Additionally, there is a very high probability of recovery from an AACS memory chip failure.

4.4.2.6 Structural Failure. As indicated in Section 3.4.1.5, there is no credible structural failure which could cause a ΔV which would lead to an Earth impacting trajectory.

4.4.2.7 AACS Software Errors. Same comments as Sections 4.4.2.3 and 4.4.2.5.

4.4.2.8 CDS Software Errors. Same comments as Sections 4.4.2.3 and 4.4.2.5.

4.4.2.9 Offsun Thermal Failure. The possibility of this failure has prompted the Galileo Project to fit the propulsion system tanks with pressure relief valves which will vent the tank contents (until nominal pressure has been achieved) in a controlled fashion with no net ΔV in the event of over-pressurization from thermal (or any other) causes. This practically eliminated the probability of an impacting trajectory due to this failure and, consequently, it was not necessary for it to influence the aimpoint biasing strategy.

4.4.2.9 Micrometeoroid Impact. Based on the analysis in Section 3, impact with interplanetary material (micrometeoroids) is the most serious problem that the Galileo spacecraft faces with regard to Earth impact. The difficulty is that if a collision occurs with sufficient energy to rupture a propellant tank, there is a significant possibility of a ΔV resulting with no reliable recovery mechanism. As a result, this particular failure dominates the impact probability numbers, as well as the navigation strategy. As discussed in Section 3.4.2.1, the micrometeoroid models have been divided into three categories: cometary meteoroids, asteroidal meteoroids, and near-Earth debris.

Regardless of the source of the impacting material, the resulting ΔV is statistically characterized by the same two densities depending upon whether or not there is one or more damaged tanks (Figure 4-8). In the case of a single tank failure, the maximum ΔV is 3.2 m/s while in the case of a multiple tank failure, the density is log normal with 90% of the ΔV expected to be less than 3.8 m/s (Section A.2.1).

The most probable spacecraft failure due to the three sources of impacting material occurs in the asteroid zone. The asteroidal material is distributed entirely within the asteroid region through which the spacecraft passes between 1.8 and 2.7 years mission elapsed time (MET). The probability of being struck by an asteroidal component large enough to cause tank rupture is 4.5×10^{-4}. Even if only 1% of the velocities resulting from this type of impact could lead to an impacting trajectory, there would still be a 4.5×10^{-6} probability of impact from this source alone. This is unacceptably high and measures have been taken to reduce it. The solution is to design the Earth 1 to Earth 2 trajectory to not be susceptible to this failure. Since micrometeoroid impacts can cause in the vicinity of 3 m/s of ΔV, the idea is to make sure that while the spacecraft is in the asteroid region, the targeted Earth 2 aimpoint will be outside of a 3 m/s vulnerability region. Figure 4-9 illustrates this constraint region. At all times that the spacecraft is in the asteroid region, the Earth 2 targeted aimpoint must be outside the region.

The cometary material is assumed to be uniformly distributed in the regions of the solar system between launch and EGA2. The models in Section 3.4.2.1 predict a 9.1×10^{-6} probability of failure of the RPM tanks by the time of EGA2 which is 7.8×10^{-9} per day. After accommodating the asteroidal micrometeoroids as above and targeting according to the third ground rule, the total contribution to the probability of Earth impact from the deep space material (cometary and asteroidal micrometeoroids) will be on the order of 4×10^{-7} using the upper bound models developed here.

As far as Earth avoidance is concerned, there is no danger from near-Earth debris. Referring to Figure A-15, near-Earth debris is only present during the final 15 minutes before the flyby. As shown in Figure 4-10, by the time the Galileo spacecraft is within this range the ΔV required to achieve impact is well over 100 m/s which is well beyond the capability of any possible failure mode involving collision with debris.

4.4.2.10 Radiation-SEU Effects. The effect of this failure is identical to an AACS memory chip failure.

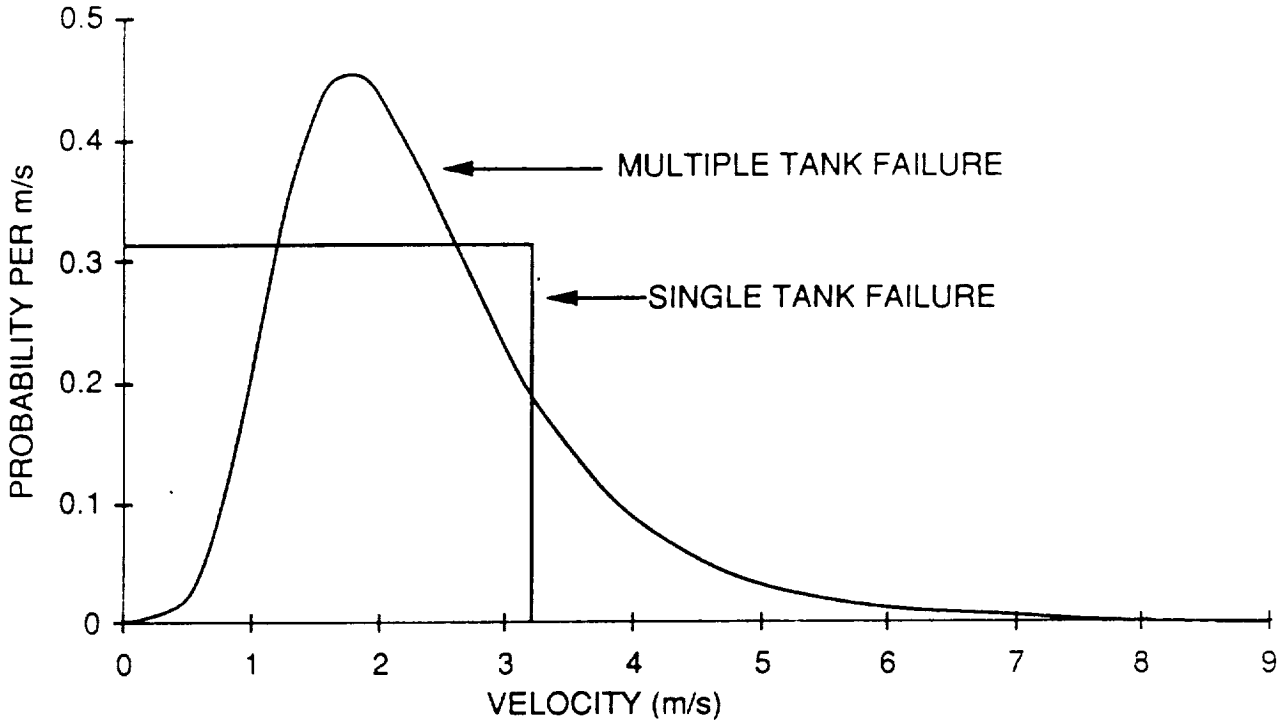


Figure 4-8. Density Function of the Velocity Distribution From a Tank Rupture

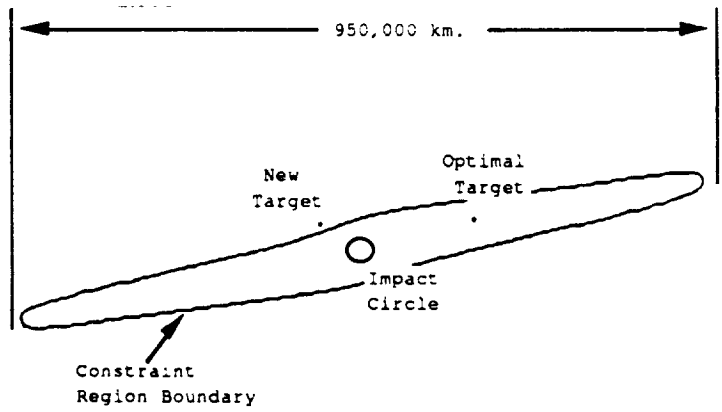


Figure 4-9. Three m/s Asteroidal Micrometeoroid Constraint Region

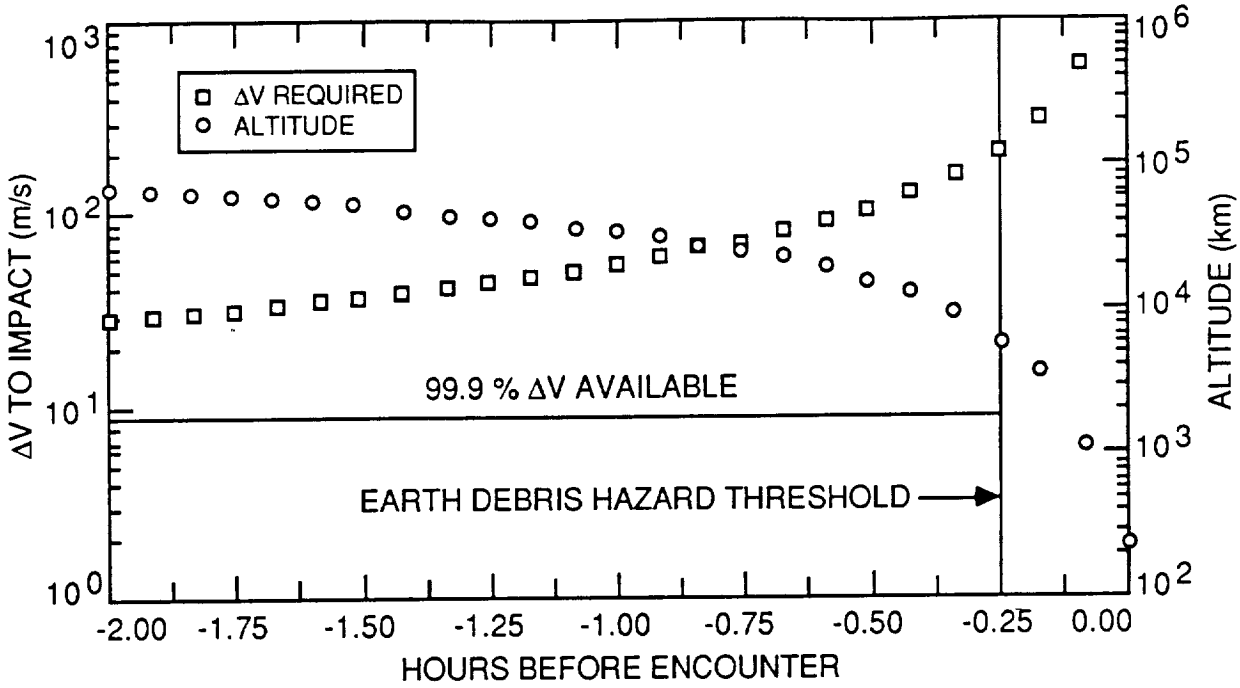


Figure 4-10. Altitude and Minimum ΔV to Impact at 300 Kilometers

4.4.2.11 Spacecraft Charging. This failure can only affect the first TCM after Earth 1 and can only cause a lateral burn in the wrong direction. At this point in the mission, the spacecraft is targeted approximately 1×10^6 km from Earth and there is virtually no possibility of an erroneous burn causing an impacting trajectory. Taking the very worst case of 50% of the spurious ΔVs causing an impacting trajectory would lead to a probability of impact of 1.2×10^{-9}.

4.4.2.12 Command Generation Process. With all failures of this type, there is a very high probability of recovery since there are no spacecraft hardware failures to hinder recovery procedures. This, combined with the internal and external checks in the command generation process system makes the probability of such an event extremely remote. A very conservative upper bound on the probability of impact from this failure is 1.3×10^{-7}.

4.4.2.13 Uplink Command Errors. As indicated in Section A.3.2, the probability of such an event is less than 1×10^{-17} and is not considered.

4.5 A PARTICULAR CASE: THE OCTOBER 9, 1989 LAUNCH

Clearly the precise implementation of the considerations and criteria listed above will depend upon the particular trajectory which in turn depends upon launch date and other criteria. Additionally, the Earth avoidance strategy must be adaptive to slight changes in the spacecraft trajectory due to nominal dispersions. Thus the target parameters presented here will necessarily be representative and not final. The final aimpoint determination will be done in flight in response to trajectory variations. However, all groundrules will be followed and thus the total impact probability as presented below will not change.

The 1989 launch period for Galileo extends from October 9 to November 24. During this period there are actually three distinct types of trajectories to Jupiter. During the initial portion, it is possible to design a trajectory which encounters two asteroids; Gaspra between the first and second Earth flybys, and Ida between Earth 2 and Jupiter (Figure 2.1-2). Later in the launch period, decreasing propellant margins require the removal of the Ida encounter and leave Gaspra. Even later in the period, and for the same reasons, the flyby with Gaspra is replaced with asteroid 1938SD1, also between Earth 1 and Earth 2.

For this study, the trajectory corresponding to a launch date of October 9, 1989 will be used. This is a representative trajectory and is also the most stressful in terms of Earth avoidance requirements. The design values for both the Earth flyby altitudes are as low as they ever become throughout the 1989 launch opportunity and there are additional characteristics, such as the Venus to Earth 1 trajectory characteristics (covered below), which qualify the October 9 trajectory as the most demanding in influencing the biasing strategy. The Earth avoidance strategy designed for this trajectory will produce an equal or lesser probability of inadvertent reentry for any other trajectory during the 1989 launch opportunity.

4.5.1 Trajectory Description

The major trajectory events for the October 9 launch opportunity are summarized in Table 4-3.

Table 4-3. Launch to Earth 2 Events for October 9, 1989 Launch

Date	Event	
October 9, 1989	Launch	
	C_3	17.7 km^2/s^2
February 12, 1990	Venus Flyby	
	Altitude	13896 km
December 8, 1990	First Earth Flyby	
	Altitude	970 km
	V_∞	8.99 km/s
	Flyby Velocity	13.8 km/s
October 29, 1991	Gaspra Encounter	
December 8, 1992	Second Earth Flyby	
	Altitude	303 km
	V_∞	8.88 km/s
	Flyby Velocity	14.1 km/s

4.5.2 Maneuver Profile

The maneuver profile for the the October 9, 1989 launch has been designed to ensure accurate delivery at each encounter with the most efficient use of propellant and operational simplicity, while insuring that the probability of Earth impact is made very small. Table 4-4 summarizes the maneuver profile and the main function of each maneuver.

Table 4-4. Maneuver Profile

Maneuver	Epoch (days)	Description
TCM1	Launch + 21	Clean up IUS dispersions and remove launch bias
TCM2	Launch + 50	Clean up TCM1 dispersions and remove most of TCM1's bias
TCM3	Venus - 10	Remove last of bias at Venus
TCM4	Venus + 90	Clean up Venus delivery and target to first biased aimpoint at Earth 1
TCM5	Venus + 110	Clean up for TCM4 and move aimpoint closer to Earth
TCM6	Earth - 60	Move aimpoint closer to Earth
TCM7	Earth - 25	Target to desired flyby conditions at Earth 1
TCM8	Earth - 10	Final targeting maneuver to remove last dispersions at Earth 1
TCM9	Earth + 7	Clean up dispersions resulting from Earth 1 flyby
TCM10	Earth + 71	Deep space maneuver targeting to Gaspra
TCM11	Gaspra - 20	Target to Gaspra using optical data
TCM12	Gaspra - 5	Final targeting maneuver to Gaspra using optical data
TCM13	Gaspra + 281	Post-Gaspra deep space maneuver targeting to first biased aimpoint at Earth 2
TCM14	Earth - 60	Move aimpoint closer to Earth
TCM15	Earth - 25	Target to desired flyby conditions at Earth 2
TCM16	Earth - 10	Final targeting maneuver to remove last dispersions at Earth 2

4.5.3 Parameters for Statistical Analysis

For the probabilistic analysis below, the representative values of the parameters describing the behavior of the propulsion system and the orbit determination process have been used. These are conservative estimates of expected performance based on specifications of the hardware and engineering analysis. Any deviations from this expected performance have been covered in the failure analysis of Section 3.

4.5.4 Detailed Description of Earth Avoidance Strategy

4.5.4.1 Launch to Venus. There are two principle reasons why there is no concern for a spurious ΔV causing an Earth impacting trajectory during this phase of the mission. The first is that it requires an extremely accurate delivery at Venus for the gravitational energy augmentation to alter the trajectory in the precise amount needed to effect the next Earth encounter. Without any biasing whatsoever, the probability of a spurious ΔV accomplishing this is on the order of 10^{-10}. The second reason is that the trajectory is to be biased to satisfy the first ground rule regarding normal maneuver dispersions. The result of this biasing further reduces probability of a Type II failure causing impact.

4.5.4.1.1 Injection. As mentioned in the introduction to this report, IUS malfunctions which would lead to reentry at less than Earth escape velocity are not covered in this report. These cases are treated in the Galileo Final Safety Analysis Report by the Department of Energy. There are no Earth avoidance implications if the Galileo spacecraft were to fail during the launch phase of the mission. For reasons of operational simplicity, propellant savings, and reduced cycling of the RPM P1A thruster, the decision has been made to build in a 17 m/s bias along the Sun-line into the injection target. That is, if the IUS performs perfectly, the spacecraft will still have to perform a 17 m/s burn at TCM1 to achieve the proper Venus target (Figure 4-11). While this complicates the launch vehicle targeting design, it actually simplifies concerns about Earth avoidance. In particular, this bias removes all worry about the IUS performing nominally and launching an inert Galileo spacecraft due to some failure during the launch phase. The 17 m/s bias at TCM1 translates into some 200,000 km in the Venus B-plane, which would cause the spacecraft to miss the Earth by many tens of millions of kilometers. There is no possibility of reentry in this case.

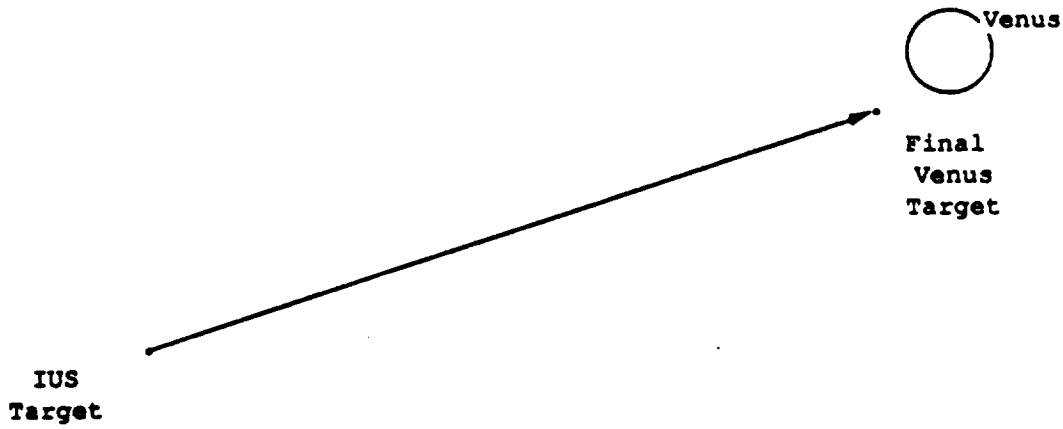


Figure 4-11. IUS Target Bias

4.5.4.1.2 Launch + 21 Days (TCM1). The impetus for biasing the TCM1 aimpoint is a Type I failure. The target at Venus must ensure that the dispersions at Venus mapped to Earth do not overlap the Earth's impact circle with a greater than 1 x 10^{-6} probability. If TCM1 targets directly to the design value for the Venus aimpoint, then the dispersions mapped to Earth yield an a priori probability of a post-maneuver impacting trajectory of 3 x 10^{-5}, well above the ground rule value of 1 x 10^{-6} It is necessary to bias the aimpoint at Venus to reduce this probability. Two thousand kilometers in the Venus B-plane is more than sufficient. This bias is chosen to lie along the Earth negative b•T gradient direction (Figure 4-12). The result is that the Earth aimpoint will be shifted over 21 million kilometers, primarily in the negative b•T direction. This will reduce the probability of navigation dispersions resulting in an impacting trajectory to an insignificant amount (1 x 10^{-22}).

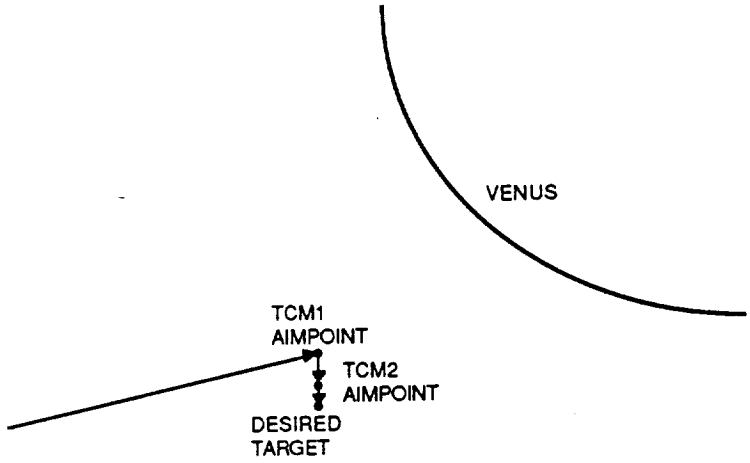


Figure 4-12. Biases of TCM1 and TCM2

4.5.4.1.3 Launch + 50 Days (TCM2). Exactly the same criterion that applied to TCM1 applies to TCM2. The only difference is that now the dispersions mapped from Venus to Earth are much smaller. This results from smaller orbit determination errors, but is primarily based on the fact that TCM2 is a very small clean up maneuver for TCM1 and, thus, has much smaller execution errors. However, there still must be a bias in the aimpoint. If there were no bias, the probability of achieving an impacting trajectory would be 2 x 10^{-5}. A sufficient bias to keep out of the 1 x 10^{-6} zone is 100 kilometers. With this bias, the probability is 2 x 10^{-11}.

4.5.4.1.4 Venus - 10 Days (TCM3). TCM3 is the final targeting maneuver before Venus. The maneuver removes the last of the bias left by TCM2 as well as any execution and orbit determination errors. With the built-in bias at Earth 1, the probability of an impacting trajectory resulting from navigation dispersions is 3 x 10^{-10}.

4.5.4.2 Venus to EGA1. As mentioned in Section 4.5.4.1, the Venus aimpoint is chosen so that the post-Venus trajectory to Earth will be targeted at a sufficiently large distance to satisfy the 1 x 10^{-6} navigation dispersions criterion (Rule 1) (Figure 4-13).

Figure 4-13. Post-Venus and Final Earth 1 Aimpoints

For this trajectory, this amounts to over 700,000 km in the B-plane. To accurately arrive at the proper aimpoint for the Earth flyby and reduce Earth impact probabilities, there are five maneuvers. The first two are a large DSM and clean up which do most of the targeting to the final aimpoint. The next two sequentially step to the final aimpoint while satisfying the third ground rule. The final maneuver is to remove, as much as possible, the dispersions at Earth 1. The target aimpoint for Earth 1 is b = (-6648, -9073) which is equivalent to an altitude of 970 km. The aimpoints for each maneuver are illustrated in Figure 4-14.

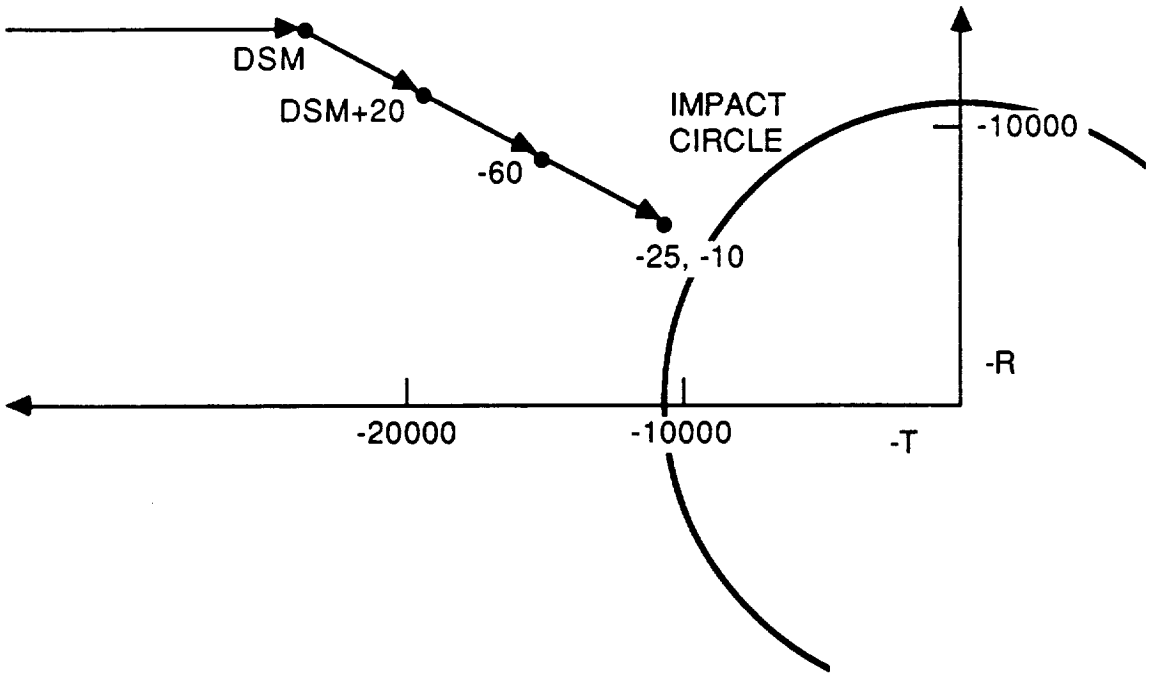


Figure 4-14. Earth 1 Aimpoints

4.5.4.2.1 Venus + 90 Days (TCM4). TCM4 does most of the work in removing the post-Venus bias. For this trajectory, the size of this maneuver is about 12m/s and is scheduled at 90 days after the Venus encounter. The strategy for this maneuver will be to target to the edge of the 1×10^{-6} contour while setting up the direction for the sequence of small maneuvers which move to the final aimpoint. The aimpoints for this and subsequent maneuvers are summarized in Table 4-5 below.

4.5.4.2.2 Venus + 110 day Maneuver (TCM5)
Earth 1 - 60 day Maneuver (TCM6)
Earth 1 - 25 day Maneuver (TCM7).

The goal of these three maneuvers is to move in radially to the final aimpoint. The targets for each of the maneuvers are summarized in Table 4-5.

4.5.4.2.3 Earth 1 - 10 day Maneuver (TCM8). TCM8 is a very small clean up maneuver to remove the last of the dispersions from TCM7 to ensure as accurate a delivery to Earth as possible.

4.5.4.2.4 Aimpoint Summary. Table 4-5 presents the actual aimpoints in the Earth B-plane. Figure 4-15 indicates the target altitude as a function of time before the Earth 1 encounter.

4.5.4.3 Earth 1 to Gaspra. There are four maneuvers planned between EGA1 and Gaspra. The first is a clean up maneuver to remove the dispersions from the Earth flyby. The second is a fairly large (8 m/s) targeting maneuver to aim at Gaspra. The final two are small TCMs which make use of optical data to accurately target to the final Gaspra aimpoint. It is not necessary to bias these maneuvers for the purposes of Earth avoidance. Because the trajectory is designed to accommodate impacts from asteroidal micrometeoroids (Section 4.4.2.8), any concern for Type I failures is also automatically removed.

Table 4-5. Earth 1 Aimpoints

Mnvr.	b•R	b•T	b	Altitude
Post Venus	-13974	-706387	706525	695230
TCM4	-12000	-15000	19209	8521
TCM5	-10018	-13673	16950	6342
TCM6	-8179	-11164	13839	3381
TCM7	-6648	-9073	11248	970
TCM8	-6648	-9073	11248	970

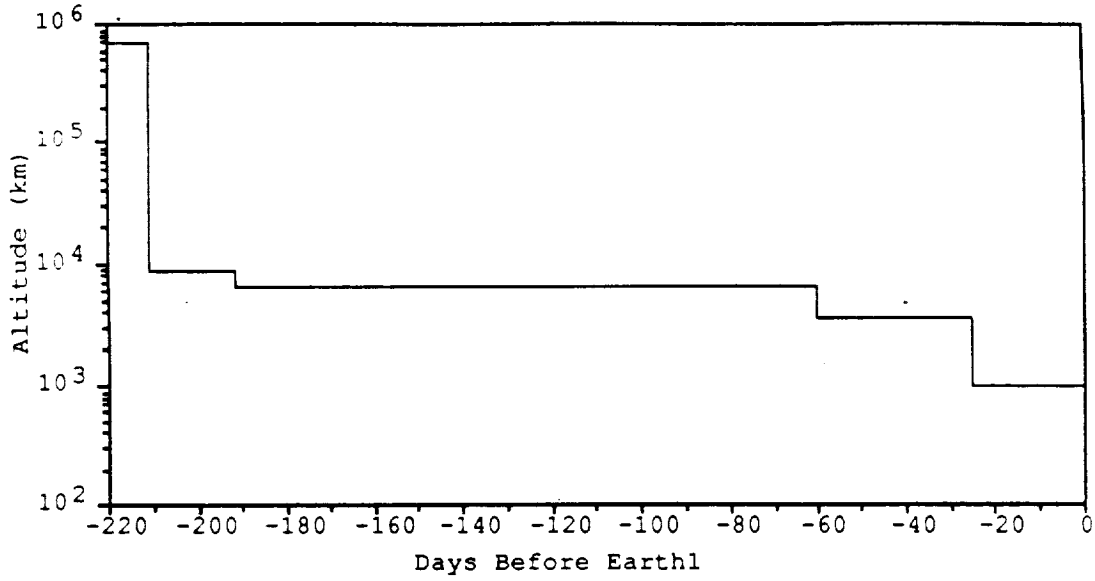


Figure 4-15. Earth 1 Targeted Altitude

After a nominal first Earth flyby, the spacecraft will be targeted over a million kilometers away from Earth 2. This, combined with the orientation of the dispersion in the Earth 2 B-plane, makes it unnecessary to make any special provisions for navigation dispersions. After the 8 m/s DSM, the Earth 2 aimpoint is still several tens of thousands of kilometers removed from the impact circle and Type I failures do not enter into the biasing strategy.

4.5.4.4 Gaspra to Earth 2. After the Gaspra flyby the spacecraft is targeted via a similar series of maneuvers, to an aimpoint as illustrated in Figure 4-16. The final aimpoint is slightly over 300 km in altitude.

There will be five maneuvers between Gaspra and Earth 2. The first will be a clean-up maneuver which will target to the nominal post-Gaspra aimpoint. The spacecraft will remain targeted to this point until such time as the danger of being struck by an asteroidal micrometeoroid has passed. For this trajectory, this occurs 125 days before EGA 2. At this point, the first of four maneuvers targeting to the final Earth 2 aimpoint begins. The final aimpoint is b = (1079, -10537), which corresponds to an altitude of 303 kilometers. The sequence of aimpoints is illustrated in Figure 4-17.

4.5.4.4.1 Earth 2 - 125 day Maneuver (TCM14). This maneuver will do the major portion of the work in moving from the post-Gaspra aimpoint to the final Earth aimpoint. Its nominal size is about 24 m/s. As with TCM4, it will target to the outside of the 1×10^{-6} ellipse while setting up the direction for the final biasing TCMs.

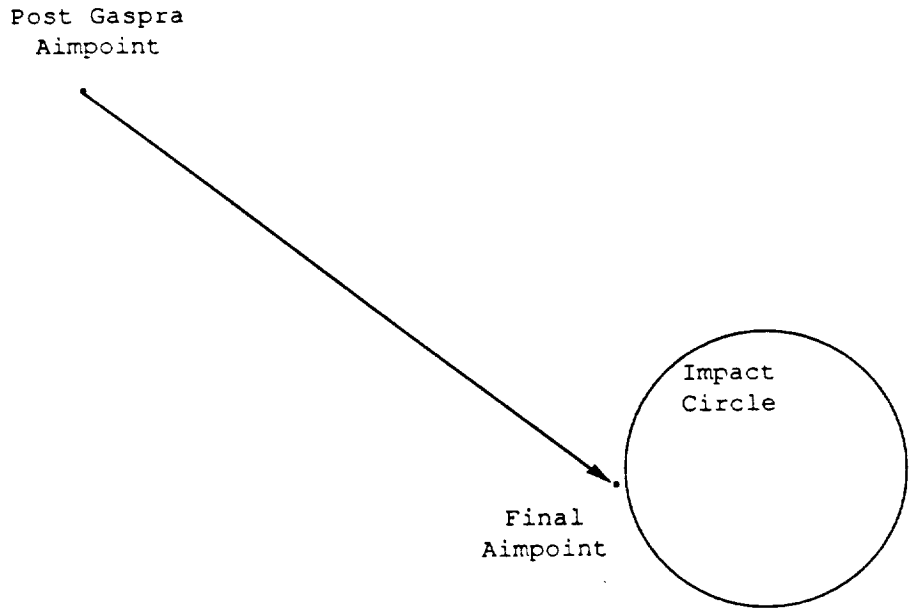


Figure 4-16. Post-Gaspra and Final Earth 2 Aimpoints

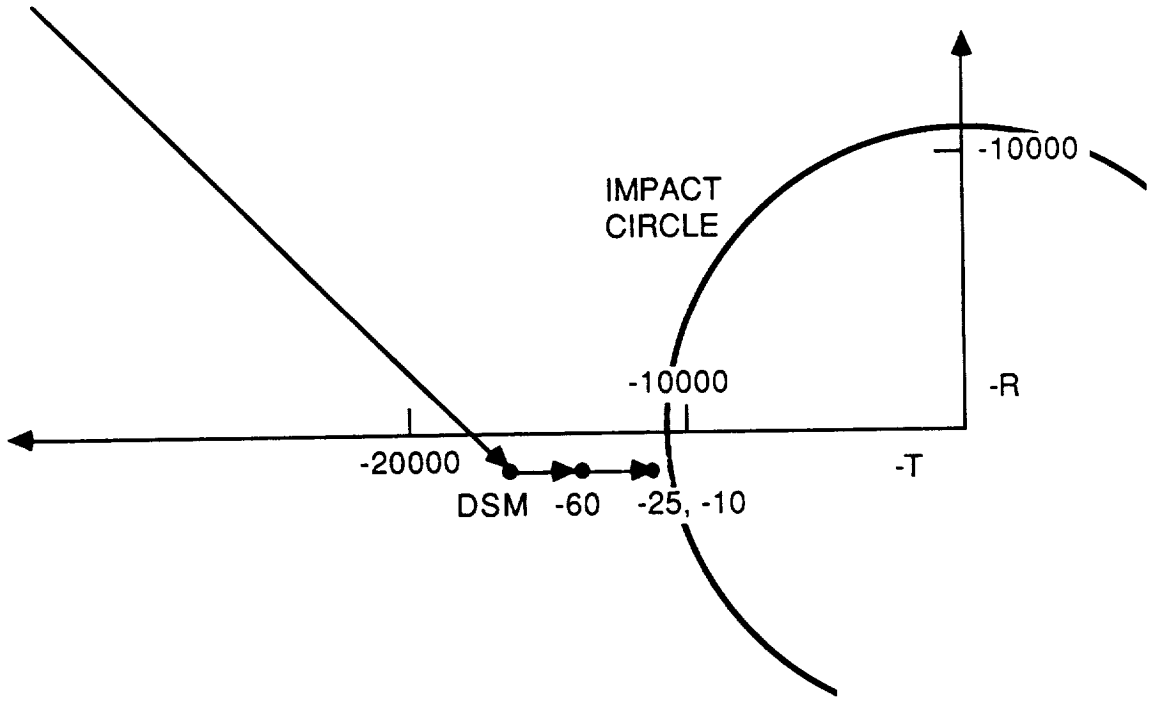


Figure 4-17. Earth 2 Aimpoints

4.5.4.4.2 Earth 2 - 60 day Maneuver (TCM 15)
Earth 2 - 25 day Maneuver (TCM 16).

The goal of these two maneuvers is to move in radially to the final aimpoint. The targets for each of the maneuvers are summarized in Table 4-6.

4.5.4.4.3 Earth 1 - 10 day Maneuver (TCM 17). TCM17 is a very small clean up maneuver to remove the last of the dispersions from TCM16 to ensure as accurate a delivery to Earth as possible.

4.5.4.4.4 Aimpoint Summary. Table 4-6 presents the actual aimpoints in the Earth B-plane and Figure 4-18 indicates the target altitude as a function of time before the Earth 2 encounter.

Table 4-6. Earth 2 Aimpoints

Maneuver	b•R	b•T	b	Altitude
Post-Gaspra	-20544	-59690	63126	51895
TCM14	1079	-16267	16304	5636
TCM15	1079	-13157	13202	2703
TCM16	1079	-10537	10592	303
TCM17	1079	-10537	10592	303

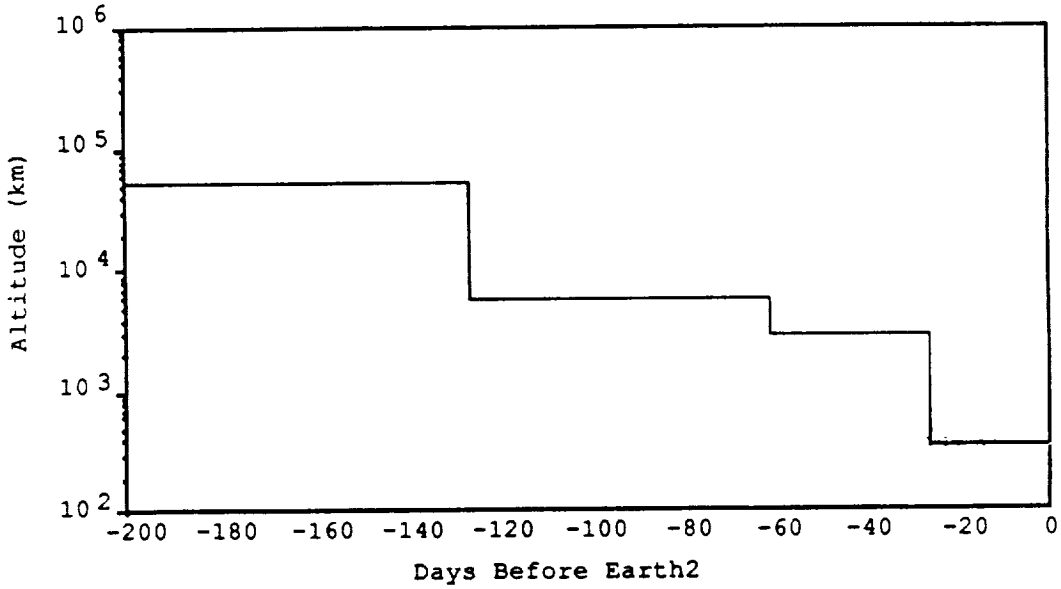


Figure 4-18. Earth 2 Targeted Altitude

4.5.5 Earth Impact Probability: Consequences of Earth Avoidance Strategy

By using the contents of Section 3.4 and the Appendix, which relate the probability of the various failure scenarios and their expected effects upon the spacecraft's trajectory together with the formulae above expressing the impact probabilities as a function of these parameters, it is possible to compute a bound for the total probability of Earth impact.

Table 4-7 contains a breakdown of the probabilities for each failure category as computed for the aimpoint design strategy above. It should be noted that in some cases, to relieve the computational burden, conservative techniques were used to estimate these probabilities. Thus, in all cases, these probabilities represent an upper bound on the probability of impact given the failure models presented above and in Section 3. The bottom line is that a best estimate upper bound on the probability of the Galileo spacecraft impacting the Earth is 5×10^{-7}.

Table 4-7. Probability of Impact Summary

Paragraph	Description	P (Impact) Earth 1	P (Impact) Earth 2
3.4.1.1	RPM Tank Failure	0.0	0.0
3.4.1.2	Stuck Thruster (Maneuver)	9.2×10^{-11}	4.4×10^{-9}
3.4.1.2	Stuck Thruster (HGA correct)	1.4×10^{-9}	0.0
3.4.1.2	Stuck Thruster (Spin correct)	3.6×10^{-10}	0.0
3.4.1.3	RPM Thruster Failure	0.0	0.0
3.4.1.4	AACS Memory Chip Failure	1.3×10^{-12}	4.3×10^{-11}
3.4.1.5	Structural Failure	0.0	0.0
3.4.1.6	AACS Programming Error	1.1×10^{-12}	3.7×10^{-11}
3.4.1.7	CDS Software Failure	3.3×10^{-11}	2.8×10^{-11}
3.4.1.8	Offsun Thermal Failure (Rupture)	3.2×10^{-10}	2.1×10^{-9}
3.4.1.8	Offsun Thermal Failure (Parts)	3.6×10^{-10}	3.6×10^{-10}
3.4.2.1	Micrometeoroid Impact	1.8×10^{-7}	1.9×10^{-7}
3.4.2.2	Radiation-SEU Effects	1.9×10^{-12}	1.9×10^{-10}
3.4.2.3	Spacecraft Charging	0.0	1.2×10^{-9}
3.4.3.1	Command Generation Process	6.0×10^{-8}	7.0×10^{-8}
3.4.3.2	Uplink Command Errors	0.0	0.0
	Totals	2.4×10^{-7}	2.7×10^{-7}
	Total Probability of Impact	5×10^{-7}	

4.6 SENSITIVITIES

Clearly the results of the previous section depend on a number of modeling assumptions and it is of interest to determine the sensitivity of the final probability of impact to these assumptions. Figure 4-19 graphically presents the data in Table 4-7. The dominant factor in the Earth impact probability is the effect of micrometeoroid impacts. As stated in Section 3.1, all of the estimates of failure probabilities are extremely conservative.

In the case of the micrometeoroids, this conservatism is compounded by the use of the Galileo model for cometary micrometeoroids as opposed to the NASA model and by the inclusion of the model for asteroidal micrometeoroids. If the NASA model were used instead, the probability of impact contribution from micrometeoroids is reduced by a factor of three. This would yield a total probability of impact of 2.7×10^{-7}.

The next most dominant effects are the command generation process and the stuck thrusters. There is a great deal of conservatism in the estimation of errors in the command generation process and as mentioned in Section 3.4.1.2, the analysis of stuck thrusters does not take into account the addition of the PDE annex which significantly reduces the probability of this failure occurring.

Going in the other direction, with the exception of failures which do not have a feasible recovery mechanism (such as micrometeoroid impacts), the probability of recovery plays a central role in determining the probability of impact. Throughout this report, the value of a 1% probability of a half subsystem failure has been used as a factor in determining the recovery probability. As a test of the sensitivity of the probability of impact to this rate, an analysis of the actual part failure rates observed for the two Voyager spacecraft has been performed. If the results of this analysis are appled to Galileo, a half subsystem failure rate of 5% is obtained. (See Section 1.3.3 for a discussion of this result.) Repeating the calculations exactly as in 4.5.5 with a 5% subsystem failure rate yields a total probability of impact of 7.5×10^{-7}. The results of this analysis are presented in Figure 4-20. A much more conservative estimate of recovery probability has increased the probability of impact by a relatively small amount.

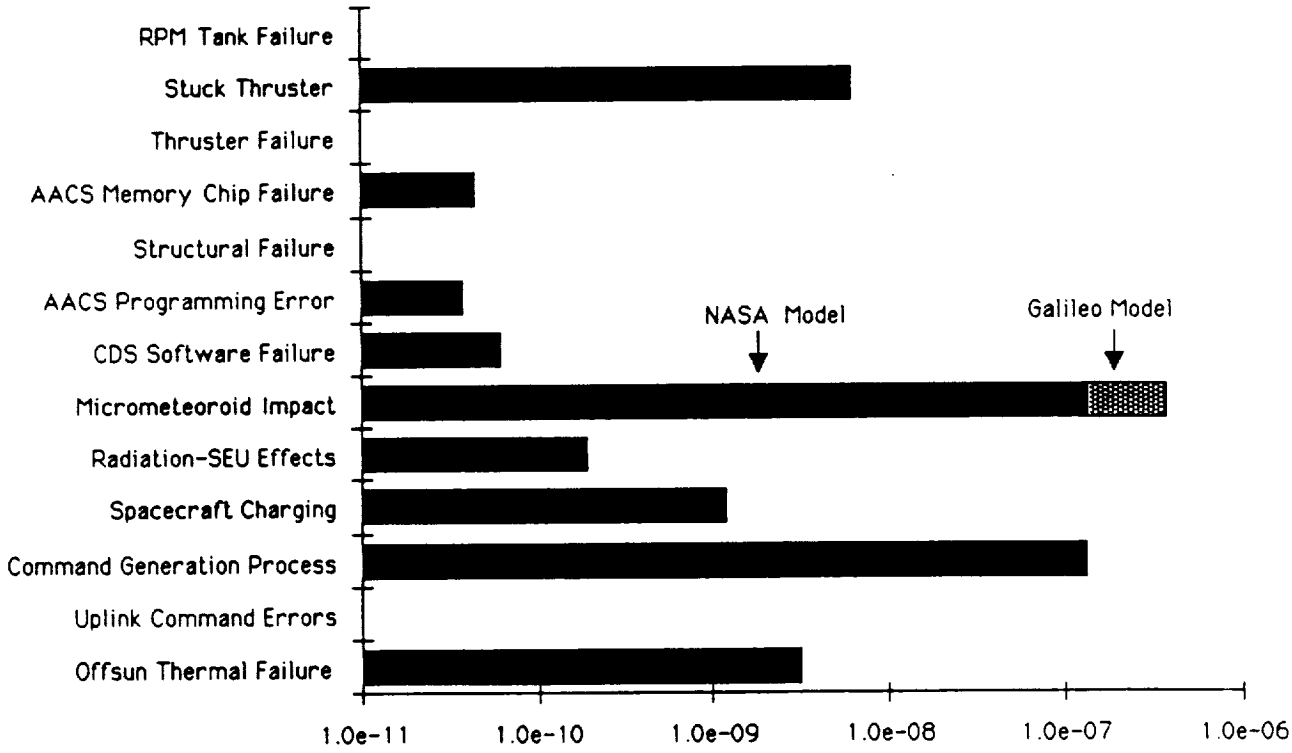


Figure 4-19. Earth Impact Probabilities Summary

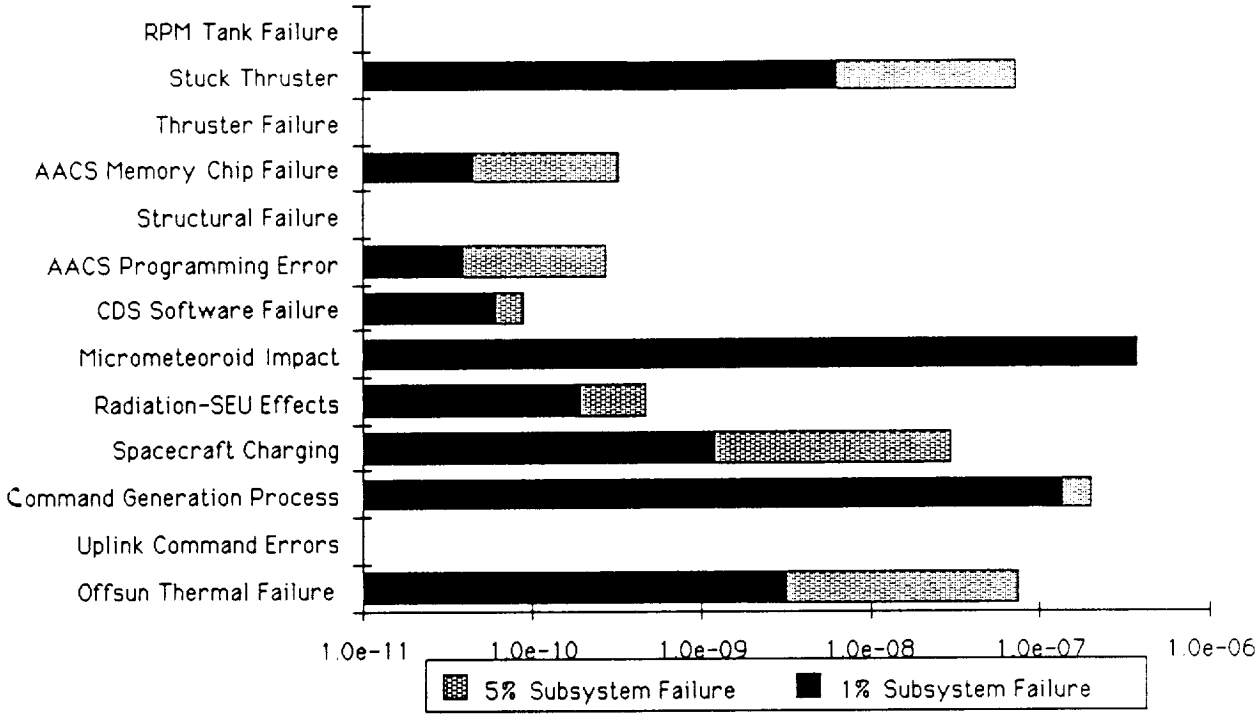


Figure 4-20. Earth Impact Probabilities Summary for 5% Half Subsystem Failure Rate and Galileo Micrometeoroid Model

As a final note, it is informative to compare the probability of a failure occurring with the actual probability of that failure causing Earth impact. Table 4-8 presents such a summary. The navigation strategy, in conjunction with the high reliability of the spacecraft and its ability to recover from most failures, reduces the probability of any failure actually causing Earth impact by several orders of magnitude and has made the probability of inadvertent Earth reentry extremely remote.

Table 4-8. Probabilities of Earth Reentry by Failure Mode

Failure Mode	Probability of Failure	Probability of Earth Reentry
Micrometeoroid Impact	4.5×10^{-4}	3.7×10^{-7}
Command Generation	5.0×10^{-3}	1.3×10^{-7}
Stuck Thruster	6.5×10^{-2}	6.3×10^{-9}
Thermal Failure	1.5×10^{-6}	3.1×10^{-9}
Spacecraft Charging	1.2×10^{-3}	1.2×10^{-9}
Radiation-SEU Effects	1.0×10^{-4}	1.9×10^{-10}
Software Failure	4.3×10^{-5}	6.1×10^{-11}
AACS Chip Failure	7.0×10^{-5}	4.4×10^{-11}

APPENDIX

FAILURE MODES ANALYSIS

This Appendix describes in detail the analysis that was done for each of the failure modes summarized in Section 3. The organization is the same as Section 3; there is a Section devoted to each of the failures in the same order and with the same numbering system used in Section 3. The derivation of the standard probability of recovery values is at the end of this Appendix.

A.1 Spacecraft Failures

A.1.1 Propellant Line or Tank Ruptures

The failure mode considered here includes any hardware failure in the Retro Propulsion Module (RPM) which lead to escaping propellants or pressurant and results in an anomalous velocity imparted to the spacecraft. Failures in the electronics which drive the RPM thrusters and latch valves (also known as isolation valves or isovalves) are not included in this category; they are covered in Section A.1.4. Failures in the software that commands the electronics which drive the RPM are similarly covered in Sections A.1.6 and A.1.7.

In analyzing the hardware failure modes of the RPM itself, it was discovered that by far the most likely failure mechanism was due to impact of RPM components by a micrometeoroid. No structural failure of propellant tanks or lines inherent in the hardware itself even came close to the chance of tank penetration by a solid or liquified micrometeoroid. This failure category is analyzed in great detail in Section A.2.1 as one of the environmentally induced failure categories. The analysis of this failure mode is left to that Section.

A.1.2 Stuck Thrusters

The failure mode under consideration here is where a stuck open or stuck closed thruster valve causes an anomalous velocity increment to be applied to the spacecraft. This is only a concern during a maneuver since only then are the isovalves opened. In this category the cause of the failure is a hardware failure in the thruster valve, the propulsion drive electronics (PDE), or the PDE annex. Other hardware and software failures which might cause anomalous thruster firings are covered in Sections A.1.4, A.1.6, and A.1.7.

Figure A-1 shows the orientation and nomenclature of the twelve 10 N thrusters. Note that each thruster designation indicates 'A' or 'B' plumbing branch, and thruster cluster number 1 or 2. Figure A-2 shows a simplified schematic of the propellant tanks and plumbing. This Figure shows how the isovalves separate the 'A' and 'B' branch thrusters, and how isovalves and thruster valves must both be open before a thruster can fire. If only 'A' branch isovalves are opened, then no 'B' branch thruster can fire. Isovalves are opened only when a maneuver is about to begin, and are closed immediately upon completion.

The isovalves act as a safety net, limiting the damage that might be done by a stuck open thruster valve. An isovalve stuck open would not by

itself result in imparted velocity. In any event, an isovalve stuck shut will result in no maneuver being performed. This analysis considered both isovalves and thruster valves stuck open, but the probability of such a double failure occurring was so small that it made a negligible contribution to the total probability.

When the spacecraft is close to the Sun (near Venus), a stuck open thruster could cause off-Sun attitude excursions which result in temperature damage to the HGA. Such damage could occur before baseline fault protection responded. As a result, the addition of a sungate and a PDE annex device was made to the spacecraft specifically to guard against a stuck open thruster fault.

The Sun gate is a photoelectric sensor which triggers an on-board fault protection response whenever the HGA-Sun angle exceeds a threshold, due to some spacecraft malfunction.

The PDE annex detects and prevents an anomalous signal to a thruster valve when no signal was issued by the AACS I/O. Hence, the probability of the propulsion drive electronics (PDE) causing a stuck open thruster failure has been greatly reduced.

The analysis described in this Appendix does not consider the improved reliability of the spacecraft as a result of the addition of the sun gate and PDE annex devices, since the need for them, which is unique to the VEEGA trajectory, had not been identified when this effort began. However, since these devices have now been incorporated, the probability of a stuck thruster failure will be substantially less than that used in this analysis.

Some general remarks can be made about the effects of a stuck open thruster:

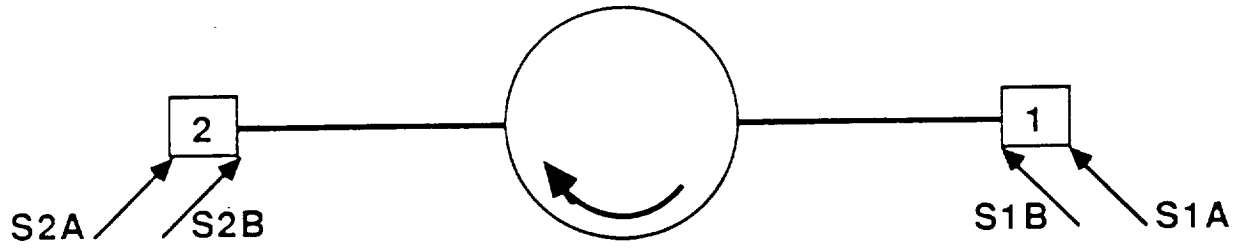
- Any S thruster stuck open will trigger AACS internal fault monitor 25 or 26 (spin rate bounds) or if in inertial mode fault monitor 3, 4, 5, or 6 (gyro rate too high) within 3 revs (one minute), causing a task abort, spin thruster swap, and a series of spin rate corrections. Net velocity imparted would be less than 0.05 m/s.

- Any Z thruster stuck open in inertial mode will trigger fault monitor 3, 4, 5, or 6 (gyro rate too high) within 3 revs (one minute), causing the entire sequence to abort immediately. An axial velocity of 0.3 m/s or less would be imparted.

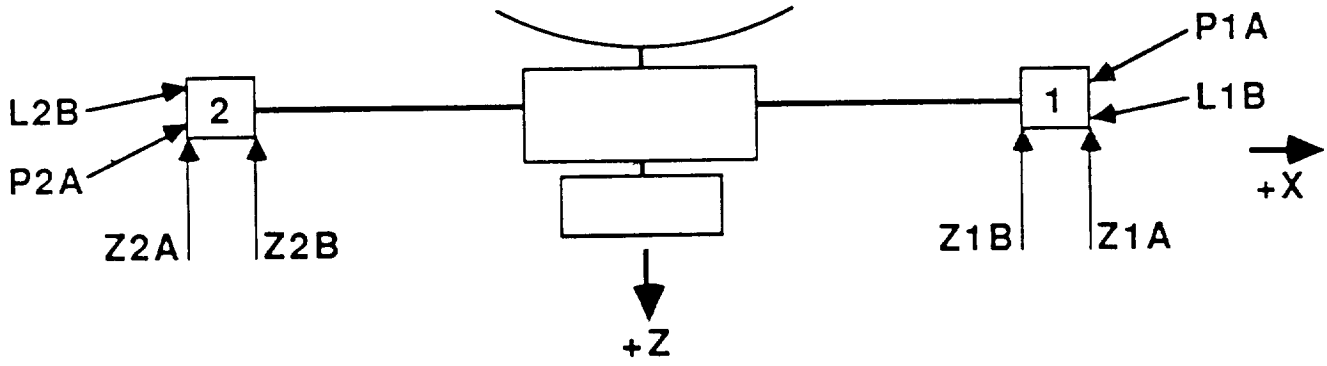
- Any P or L thruster stuck open will impart some axial velocity error; the spacecraft may be unaware of the fault and continue the sequence as if nothing was wrong.

Fault protection built into the spacecraft software will detect many stuck thruster faults. A failure in fault protection has not been considered in this analysis because:

1) The probability of such a double failure occurring is extremely small, and



SPACECRAFT TOP VIEW



SPACECRAFT SIDE VIEW

Figure A-1. Thruster Nomenclature

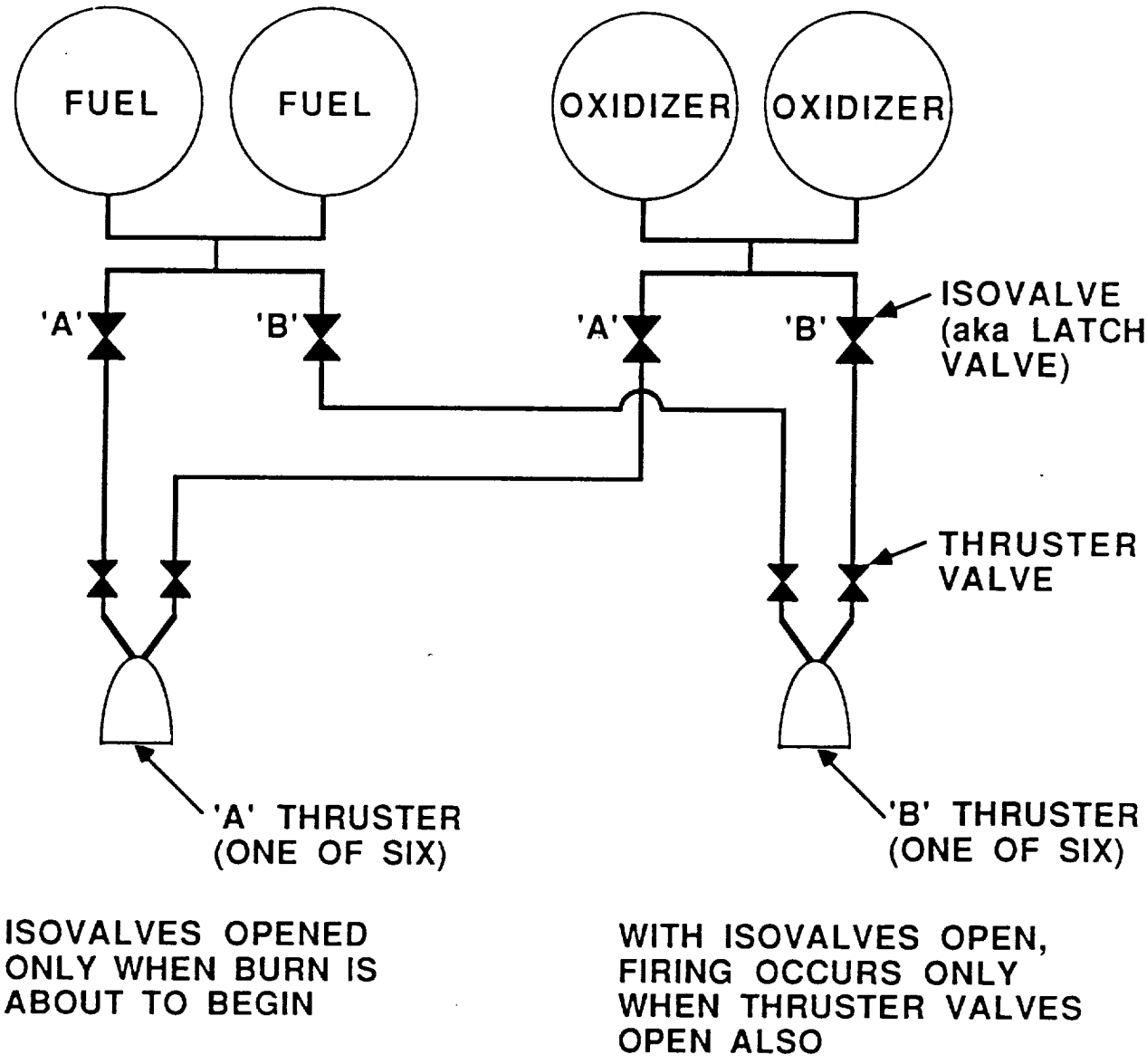


Figure A-2. RPM Valve Nomenclature and Function

2) The values used for the probability of a stuck thruster are quite large since they do not reflect the addition of new fault protection devices (sun gate and PDE annex).

Table A-1 shows which thrusters are used for each of the burn types under consideration. For example, the lateral burn uses the L1b, L2b thrusters (primary branch), with P1a, P2a as an alternate thruster choice, and is conducted in inertial mode. Then, Table A-2 summarizes the effect of all stuck thruster possibilities on each burn type. Table A-2 shows that the lateral burn, which normally uses the 'B' branch, is unaffected by any 'A' branch stuck thruster since the 'A' branch isovalves remain closed for this burn type.

An analysis of the PDE circuit components between the AACS I/O and thruster valves specified failure probabilities for two cases (W. Diem, D. Lewis, "Probability of Thruster Failure," JPL Engineering Memorandum 343-1080, 14 Dec 87):

- 'A' or 'B' branch isovalves open,
- 'A' and 'B' branch isovalves open.

Table A-1. Thrusters Used for Burn Types

Mnvr Type	Primary Branch	Alternate Branch	Spacecraft Mode
LAT	L1b,L2b	P1a,P2a	Inertial
POSZ	P1a	L1b	Inertial
PULZ	Z1a,Z2a	Z1b,Z2b	Inertial
NEGZ	Z1a,Z2a,Z1b,Z2b	Z1a,Z2a or Z1b,Z2b	All Spin
Sun Acq	P1a,P2a	L1b,L2b	All Spin
HGA Corr	P1a,P2a	L1b,L2b	All Except high spin
Spin Corr	S1a or S2a	S1b or S2b	All

The data below are for the case where PDE circuits 'A' and 'B' are both powered (normal operation). If only the PDE 'A' or 'B' circuit is powered, the change in probabilities is small. Note that these are failure probabilities with no PDE annex in operation. These failure probabilities will be considerably reduced by normal operation of the PDE annex.

Type of Failure	A or B Open	A and B Open
Prob(any S stuck open, per year)	0.00663	0.0131
Prob(any Z stuck open, per year)	0.00663	0.0131
Prob(any S stuck shut, per year)	0.00697	0.0138
Prob(any Z stuck shut, per year)	0.00697	0.0138
Prob(P1 or P2 stuck open, per year)	0.00415	0.00415
Prob(L1 or L2 stuck open, per year)	0.00415	0.00415
Prob(P1 or P2 stuck shut, per year)	0.00346	0.00346
Prob(L1 or L2 stuck shut, per year)	0.00346	0.00346
Prob(either P stuck open, per year)	0.00825	0.00825
Prob(either L stuck open, per year)	0.00825	0.00825
Prob(either P stuck shut, per year)	0.00688	0.00688
Prob(either L stuck shut, per year)	0.00688	0.00688

The probability density for occurrence of this failure is taken to be uniform with time. A stuck open or closed P or stuck open Z1a or Z2a thruster will be detected by any HGA correction (Fault Monitor 33). HGA corrections will occur about once a day, so to escape detection before a TCM, these faults must arise within a day or two preceding a TCM.

Propellant flushing maneuvers will be performed to clear propellant lines of potentially damaging corrosion products. Propellant flushing maneuvers will open both 'A' and 'B' isovalves and will provide detection of any stuck open or shut thruster. During the Venus to second Earth encounter period, propellant flushing maneuvers will occur about once per month.

Between Venus and the second Earth encounter, all TCMs except two are to be vector mode maneuvers (no turns). Two maneuvers with turns are scheduled, but analysis has shown that stuck thruster faults during a turn result in a maneuver abort with no further velocity imparted.

Values for probability of recovery are obtained from Section 3.2.4. The stuck thruster failure does not preclude recovery since all propulsive maneuvers have an alternate thruster branch with independent plumbing.

A.1.2.1 Summary of Probability

Stuck Thruster During Lateral Burn. In the execution of a lateral burn, normal operation is to fire an L1b pulse, then one half rev later fire an L2b pulse. Only 'B' branch isovalves are open.

If S1b or S2b sticks open then AACS internal fault monitor 3, 4, 5, 6, 25, or 26 (gyro rate or spin rate bounds) will abort the burn within one minute and no net ΔV will be imparted.

If an L thruster sticks open, its lateral force component will average out to zero because the spacecraft is spinning, and the other L thruster will impart about half the total intended lateral velocity. However, since the stuck open thruster is firing continuously rather than in pulses, it will impart an anomalous axial velocity equal to about 0.7 times the intended lateral velocity.

If an L thruster sticks shut, the other L thruster will impart about half the total intended lateral velocity. However, it will also impart

Table A-2. Anomalous Velocities Resulting From Afflicted Thrusters in a Maneuver

Mnvr Type	Afflicted Thruster PA	LB	ZA	ZB	SA	SB
LAT		OPEN: DVZ = 0.7*V_{LAT} SHUT: DVZ = 0.1*V_{LAT}		OPEN: ABORT, DVZ = -0.3 m/s		OPEN: ABORT, DV = 0
POSZ	P1A OPEN: DVZ = 8*VNOM P2A OPEN: DVZ = -9*VNOM		OPEN: ABORT, DVZ = -0.3 m/s		OPEN: ABORT, DV = 0	
PULZ	P2A OPEN: DVZ = 3*VNOM P1A OPEN: DVZ = -3*VNOM		OPEN: ABORT, DVZ = 0		OPEN: ABORT, DV = 0	
NEGZ	OPEN: DVZ = +4%	OPEN: DVZ = 0	SHUT: DVZ = -20%	SHUT: DVZ = -20%	ABORT, DV = 0	ABORT, DV = 0
HGA CORR	OPEN: DVZ = +0.18 m/s		OPEN: DVZ = -0.5 m/s		OPEN: DV = 0	
SUN ACQ	OPEN: ABORT, DVZ = +2 m/s		OPEN: ABORT, DVZ = -6 m/s		OPEN: ABORT, DV = 0	
SPIN CORR	OPEN: DVZ = +0.14 m/s		OPEN: DVZ = -0.4 m/s		OPEN: DV = 0	

an anomalous axial velocity equal to about 0.1 times the intended lateral velocity (V_{lat}).

If Z1b or Z2b sticks open then fault monitor 3, 4, 5, or 6 (gyro rate too high) will abort the maneuver within one minute. An anomalous axial velocity of 0.3 m/s or less would be imparted.

A stuck open or closed L or Z thruster could arise undetected in the period following the last opening of the 'B' branch isovalves. The 'B' branch is planned to be opened at least once every 26 days for the propellant flushing maneuver. This period is combined with the stuck thruster failure

rate to obtain the probability of a stuck thruster. The probability of events which cause an anomalous velocity are given below. Let the intended velocity equal V_{lat}. Then:

At EGA-60 (either EGA1 or EGA2):

P = 0.00415*26/365 = 294.E-6	DVZ = $+0.7*V_{lat}$	(L1b open)
P = 0.00415*26/365 = 294.E-6	DVZ = $-0.7*V_{lat}$	(L2b open)
P = 0.00346*26/365 = 245.E-6	DVZ = $-0.1*V_{lat}$	(L1b shut)
P = 0.00346*26/365 = 245.E-6	DVZ = $+0.1*V_{lat}$	(L2b shut)
P = 0.00663*26/365 = 472.E-6	DVZ = -0.3	(Z1b or Z2b open)

Similarly at EGA-25 (either EGA1 or EGA2):

P = 294.E-6	DVZ = $+0.7*V_{lat}$	(L1b open)
P = 294.E-6	DVZ = $-0.7*V_{lat}$	(L2b open)
P = 245.E-6	DVZ = $-0.1*V_{lat}$	(L1b shut)
P = 245.E-6	DVZ = $+0.1*V_{lat}$	(L2b shut)
P = 472.E-6	DVZ = -0.3	(Z1b or Z2b open)

At EGA-10 (either EGA1 or EGA2) the vulnerable period during which the failure may arise is 25-10=15 days:

P = 171.E-6	DVZ = $+0.7*V_{lat}$	(L1b open)
P = 171.E-6	DVZ = $-0.7*V_{lat}$	(L2b open)
P = 142.E-6	DVZ = $-0.1*V_{lat}$	(L1b shut)
P = 142.E-6	DVZ = $+0.1*V_{lat}$	(L2b shut)
P = 272.E-6	DVZ = -0.3	(Z1b or Z2b open)

These data are summarized in Table A-3.

Stuck Thruster During POSZ Burn. For a burn in the positive Z direction, normal operation is to fire a P1a pulse every one half rev.

If S1a or S2a sticks open then fault monitor 3, 4, 5, 6, 25, or 26 (gyro rate or spin rate bounds) will abort the burn within one minute and no net ΔV will be imparted.

If a P thruster sticks open, its lateral force component will average out to zero because the spacecraft is spinning, but it will impart an anomalous axial velocity equal to about 9 times the intended axial velocity.

If either P thruster sticks shut, no velocity is imparted.

If Z1a or Z2a sticks open then fault monitor 3, 4, 5, or 6 (gyro rate too high) will abort the maneuver within one minute. An anomalous axial velocity of 0.3 m/s or less would be imparted.

HGA correction maneuvers will detect a stuck open P or Z thruster. A conservative approach is to assume that there have been no HGA corrections for 2 days before each TCM. This period is combined with the stuck thruster failure rate to obtain the probability of a stuck thruster. The probability of events causing an anomalous velocity are given below, where V_{nom} equals the intended velocity.

Table A-3. Lateral Burn Probability of Failure due to Stuck Thruster and Resulting in the following ΔV During the Following Mission Phases

		$0.1 \times V_{LAT}$	0.3 m/s	$0.7 \times V_{LAT}$
AT EGA - 60				
AXIAL + Z	$0° < \theta < 30°$	245×10^{-6}		294×10^{-6}
MIXED	$30° < \theta < 60°$			
LATERAL	$60° < \theta < 120°$			
MIXED	$120° < \theta < 150°$			
AXIAL - Z	$150° < \theta < 180°$	245×10^{-6}	472×10^{-6}	294×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 25				
AXIAL + Z	$0° < \theta < 30°$	245×10^{-6}		294×10^{-6}
MIXED	$30° < \theta < 60°$			
LATERAL	$60° < \theta < 120°$			
MIXED	$120° < \theta < 150°$			
AXIAL - Z	$150° < \theta < 180°$	245×10^{-6}	472×10^{-6}	294×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 10				
AXIAL+ Z	$0° < \theta < 30°$	142×10^{-6}		171×10^{-6}
MIXED	$30° < \theta < 60°$			
LATERAL	$60° < \theta < 120°$			
MIXED	$120° < \theta < 150°$			
AXIAL - Z	$150° < \theta < 180°$	142×10^{-6}	272×10^{-6}	171×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4}

At EGA1-60 and at EGA2-60:

P = 0.00415*2/365 = 22.E-6 DVZ = +8.*V_{nom} (P1a open)
P = 0.00415*2/365 = 22.E-6 DVZ = -9.*V_{nom} (P2a open)
P = 0.00663*2/365 = 36.E-6 DVZ = -0.3 (Z1a or Z2a open)

Similarly at EGA1-25 and at EGA2-25:

P = 22.E-6 DVZ = +8.*V_{nom} (P1a open)
P = 22.E-6 DVZ = -9.*V_{nom} (P2a open)
P = 36.E-6 DVZ = -0.3 (Z1a or Z2a open)

Similarly at EGA1-10 and at EGA2-10:

P = 22.E-6 DVZ = +8.*V_{nom} (P1a open)
P = 22.E-6 DVZ = -9.*V_{nom} (P2a open)
P = 36.E-6 DVZ = -0.3 (Z1a or Z2a open)

These data are summarized in Table A-4.

Stuck Thruster During PULZ Burn. Normal operation for a pulsed burn in the -Z direction is to fire Z1a and Z2a pulses together. One half rev later, fire Z1a and Z2a pulses again.

If S1a or S2a sticks open then fault monitor 3, 4, 5, 6, 25, or 26 (gyro rate or spin rate bounds) will abort the burn within one minute and no net ΔV will be imparted.

If a P thruster sticks open, its lateral force component will average out to zero because the spacecraft is spinning, but it will impart an anomalous axial velocity such that the total axial velocity imparted is:

DVZ = +3.*V_{nom} (P2a open)
DVZ = -3.*V_{nom} (P1a open)

If Z1a or Z2a sticks open then fault monitor 3, 4, 5, or 6 (gyro rate too high) will abort the maneuver within one minute. An axial velocity of 0.3 m/s or less in the intended direction would be imparted.

If Z1a or Z2a sticks closed then the axial velocity imparted will be smaller than intended.

HGA correction maneuvers will detect a stuck open P or Z thruster. Again a conservative situation is to assume that there have been no HGA corrections for 2 days before each TCM. This period is combined with the stuck thruster failure rate to obtain the probability of a stuck thruster. The probability of events causing anomalous velocity are given below, where V_{nom} equals the intended velocity.

In this case, -V_{nom} means velocity in the +Z direction.

Table A-4. POSZ Burn Probability of Failure Due to Stuck Thruster and Resulting in the Following ΔV During the Following Mission Phases

		0.3 m/s	9.0 x V_{NOM}
AT EGA - 60			
AXIAL + Z	0° < θ < 30°		22×10^{-6}
MIXED	30° < θ < 60°		
LATERAL	60° < θ < 120°		
MIXED	120° < θ < 150°		
AXIAL - Z	150° < θ < 180°	36×10^{-6}	22×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 25			
AXIAL + Z	0° < θ < 30°		22×10^{-6}
MIXED	30° < θ < 60°		
LATERAL	60° < θ < 120°		
MIXED	120° < θ < 150°		
AXIAL - Z	150° < θ < 180°	36×10^{-6}	22×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 10			
AXIAL + Z	0° < θ < 30°		22×10^{-6}
MIXED	30° < θ < 60°		
LATERAL	60° < θ < 120°		
MIXED	120° < θ < 150°		
AXIAL - Z	150° < θ < 180°	36×10^{-6}	22×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4}

At EGA1-60 and at EGA2-60:

P = 0.00415*2/365 = 22.6E-6	DVZ = $-3.*V_{nom}$	(P1a open)
P = 0.00415*2/365 = 22.6E-6	DVZ = $+3.*V_{nom}$	(P2a open)
P = 0.00663*2/365 = 36.0E-6	DVZ = 0	(Z1a or Z2a open, task aborted with a small ΔV imparted in the intended direction.

Similarly at EGA1-25 and at EGA2-25:

P = 22.6E-6	DVZ = $-3.*V_{nom}$	(P1a open)
P = 22.6E-6	DVZ = $+3.*V_{nom}$	(P2a open)
P = 36.0E-6	DVZ = 0	(Z1a or Z2a open, see note above)

Similarly at EGA1-10 and at EGA2-10:

P = 22.6E-6	DVZ = $-3.*V_{nom}$	(P2a open)
P = 22.6E-6	DVZ = $-3.*V_{nom}$	(P1a open)
P = 36.0E-6	DVZ = -0.3	(Z1a or Z2a open)

These data are summarized in Table A-5.

Stuck Thruster During NEGZ Burn. For a continuous burn in the -Z direction, normal operation is to fire Z1a, Z2a, Z1b, Z2b continuously in the all-spin mode. Integrating accelerometers monitor accumulated axial velocity, providing closed-loop control of burn cutoff. A minimum burn time and a maximum burn time are also specified which override the accelerometer cutoff control. Commanded maximum and minimum burn times are normally set at predicted ± 5%. This ensures that a large burn error cannot occur even if the accelerometer-based burn cutoff algorithm failed.

If any S thruster sticks open, fault monitor 23 or 24 (spin rate bounds) will abort the burn within a minute with no net ΔV.

If an L thruster sticks open, accelerometer cutoff is still achieved within max/min burn times and no velocity error occurs. A P thruster stuck open would impart axial velocity and cutoff would occur at max or min time. The total axial velocity imparted would be:

DVZ = $1.04*V_{nom}$	(P2a open)
DVZ = $0.96*V_{nom}$	(P1a open)

The 'B' branch isovalves are opened less than one second before the axial ΔV estimator is initialized, and 'A' branch isovalves are opened 20 sec earlier. The 'B' branch isovalves are closed 20 sec after burn completion, and 'A' branch isovalves are closed 20 sec earlier. Hence, for any Z thruster stuck open there would be a 20 sec overburn.

Any Z stuck open: DVZ = -0.08 m/s

If any Z thruster were stuck shut, cutoff would occur at max time before achieving the intended velocity.

Table A-5. PULZ Burn Probability of Failure Due to Stuck Thruster and Resulting in the Following ΔV During the Following Mission Phases

		0.3 m/s	3.0 x V_{NOM}
AT EGA - 60			
AXIAL+Z	$0° < \theta < 30°$		22.6×10^{-6}
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$		22.6×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 25			
AXIAL + Z	$0° < \theta < 30°$		22.6×10^{-6}
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$		22.6×10^{-6}

PRABABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 10			
AXIAL + Z	$0° < \theta < 30°$		22.6×10^{-6}
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	36.0×10^{-6}	22.6×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4}

Any Z stuck shut: $DVZ = 0.8*V_{nom}$

Consider only those faults which cause more than the intended velocity. Note that the continuous -Z burn would not be chosen for very small TCMs such as the ones at ten days before each encounter.

A stuck open or shut 'B' branch thruster condition could arise undetected in the period following the last opening of the 'B' branch isovalves. The 'B' branch will be opened at least once every 26 days for the propellant flushing maneuver. A stuck 'A' branch thruster would be detected by HGA correction maneuvers which will occur at least once every two days. These periods are combined with the stuck thruster failure rates to obtain the probability of a stuck thruster. The probability of events which cause an anomalous velocity are given below. Let the intended velocity be denoted V_{nom}. Then the probability of a velocity error DVZ is:

At EGA-60 (either EGA1 or EGA2):

P = 0.00415*2/365 = 22.6E-6	$DVZ = 0.04*V_{nom}$	(P2a open)
P = 0.00663*2/365 = 36.0E-6	DVZ = -0.08 m/s	(Z1a or Z2a open)
P = 0.00663*26/365 = 472.E-6	DVZ = -0.08 m/s	(Z1b or Z2b open)

Similarly at EGA-25 (either EGA1 or EGA2):

P = 22.6E-6	$DVZ = 0.04*V_{nom}$	(P2a open)
P = 36.0E-6	DVZ = -0.08 m/s	(Z1a or Z2a open)
P = 472.E-6	DVZ = -0.08 m/s	(Z1b or Z2b open)

The NEGZ burn would not be used for small maneuvers such as at EGA-10. These data are summarized in Table A-6.

Stuck Thruster During HGA Correction. Normal operation for high gain antenna pointing maneuvers is to fire P1a and P2a pulses together once per rev. HGA corrections will occur about daily during the early cruise phase of the mission. The isovalves are open for a maximum of 100 sec.

Any 'A' branch thruster open or P1a or P2a closed means the commanded attitude will not be achieved with sufficient accuracy and fault monitor 33 (HGA error) will close the isovalves, swap the HGA thruster branch, and restart the star-based attitude determination process. This fault sequence serves as an early warning for a stuck thruster on the A Branch.

S1a or S2a open: no net velocity
Z1a or Z2a open: axial DV = -0.5 m/s
P1a or P2a open: axial DV = $\pm$0.18 m/s

The stuck thruster failure rates are used to obtain the probability of a stuck thruster at any time in the periods preceding each encounter. The probability of events which cause an anomalous velocity are given below.

From Venus flyby to EGA1-25:

P = 0.00663*275/365 = 4995.E-6	DVZ = -0.5	(Z1a or Z2a open)
P = 0.00415*275/365 = 3126.E-6	DVZ = 0.18	(P1a open)
P = 0.00415*275/365 = 3126.E-6	DVZ = -0.18	(P2a open)

Table A-6. NEGZ Burn Probability of Failure due to Stuck Thruster and Resulting in the Following ΔV During the Following Mission Phases

		0.04 x V_{NOM}	0.08 m/s
AT EGA - 60			
AXIAL + Z	0° < θ < 30°		
MIXED	30° < θ < 60°		
LATERAL	60° < θ < 120°		
MIXED	120° < θ < 150°		
AXIAL - Z	150° < θ < 180°	22.6×10^{-6}	472×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 25			
AXIAL + Z	0° < θ < 30°		
MIXED	30° < θ < 60°		
LATERAL	60° < θ < 120°		
MIXED	120° < θ < 150°		
AXIAL - Z	150° < θ < 180°	22.6×10^{-6}	472×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

From aphelion maneuver to EGA2-25:

P = 0.00663*335/365 = 6085.E-6 DVZ = -0.5 (Z1a or Z2a open)
P = 0.00415*335/365 = 3808.E-6 DVZ = 0.18 (P1a open)
P = 0.00415*335/365 = 3808.E-6 DVZ = -0.18 (P2a open)

From EGA-25 to EGA-5 (either EGA1 or EGA2):

P = 0.00663*20/365 = 363.E-6 DVZ = -0.5 (Z1a or Z2a open)
P = 0.00415*20/365 = 227.E-6 DVZ= 0.18 (P1a open)
P = 0.00415*20/365 = 227.E-6 DVZ = -0.18 (P2a open)

From EGA-5 to EGA (either EGA1 or EGA2):

P = 0.00663*5/365 = 91.E-6 DVZ = -0.5 (Z1a or Z2a open)
P = 0.00415*5/365 = 57.E-6 DVZ = 0.18 (P1a open)
P = 0.00415*5/365 = 57.E-6 DVZ = -0.18 (P2a open)

These data are summarized in Tables A-7 and A-8.

Stuck Thruster During Spin-Rate Correction. Normal operation for spin rate correction maneuvers is to fire two pulses, one half rev apart, from either S1a or S2a for spin down or spin up, respectively. This maneuver is expected to occur about once every 18 days.

If S1a or S2a stuck open or closed, the commanded spin rate would not be achieved with sufficient accuracy. Fault monitor 32 (spin-rate error) would trip and re-try spin rate correction with the other thruster branch and hence no net velocity would result.

Any other 'A' branch thruster open may trigger fault protection in inertial mode (gyro rate too high), but not in cruise mode. In this case, some axial ΔV will occur (isovalves are open for 80 sec, max).

The stuck thruster failure rates are used to obtain the probability of a stuck thruster condition arising during the approach to EGA1 and EGA2. The probability of events which cause an anomalous velocity are given below.

From Venus flyby to EGA1-25:

P = 0.00663*275/365 = 4995.E-6 DVZ = -0.4 (Z1a or Z2a open)
P = 0.00415*275/365 = 3126.E-6 DVZ = 0.14 (P1a open)
P = 0.00415*275/365 = 3126.E-6 DVZ = -0.14 (P2a open)

From aphelion maneuver to EGA2-25:

P = 0.00663*335/365 = 6085.E-6 DVZ = -0.4 (Z1a or Z2a open)
P = 0.00415*335/365 = 3808.E-6 DVZ = 0.14 (P1a open)
P = 0.00415*335/365 = 3808.E-6 DVZ = -0.14 (P2a open)

From EGA-25 to EGA-5 (either EGA1 or EGA2):

P = 0.00663*20/365 = 363.E-6 DVZ = -0.4 (Z1a or Z2a open)
P = 0.00415*20/365 = 227.E-6 DVZ = 0.14 (P1a open)
P = 0.00415*20/365 = 227.E-6 DVZ = -0.14 (P2a open)

Table A-7. HGA CORR Probability of Failure Due to Stuck Thruster at EGA1 and Resulting in the Following ΔV During the Following Mission Phases

		0.18 m/s	0.5 m/s
VENUS → EGA1 - 25			
AXIAL + Z	$0° < \theta < 30°$	3126×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	3126×10^{-6}	4995×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

EGA1 - 25 → EGA1 -5			
AXIAL + Z	$0° < \theta < 30°$	227×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	227×10^{-6}	363×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4} (EGA1- 25 to EGA1-10)
5×10^{-3} (EGA1- 10 to EGA1-5)

EGA1 - 5 → EGA1			
AXIAL + Z	$0° < \theta < 30°$	57×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	57×10^{-6}	91×10^{-6}

PROBABILITY OF NO RECOVERY = 10^{-1}

Table A-8. HGA CORR Probability of Failure Due to Stuck Thruster at EGA2 and Resulting in the Following ΔV During the Following Mission Phases

		0.18 m/s	0.5 m/s
APHELION → EGA2 - 25			
AXIAL + Z	$0° < \theta < 30°$	3808×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	3808×10^{-6}	6085×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

EGA2 - 25 → EGA2 -5			
AXIAL + Z	$0° < \theta < 30°$	227×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	227×10^{-6}	363×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4} (EGA2 - 25 to EGA2 - 10)
5×10^{-3} (EGA2 - 10 to EGA2 - 5)

EGA2 - 5 → EGA2			
AXIAL + Z	$0° < \theta < 30°$	57×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	57×10^{-6}	91×10^{-6}

PROBABILITY OF NO RECOVERY = 10^{-1}

From EGA-5 to EGA (either EGA1 or EGA2):

P = 0.00663*5/365 = 91.E-6	DVZ = -0.4	(Z1a or Z2a open)
P = 0.00415*5/365 = 57.E-6	DVZ = 0.14	(P1a open)
P = 0.00415*5/365 = 57.E-6	DVZ = -0.14	(P2a open)

These data are summarized in Tables A-9 and A-10.

Stuck Thruster During Sun Acquisition. Normal operation for Sun acquisition maneuvers is to fire the P1a and P2a pulses together once per rev. This maneuver is not planned to be used after the first TCM and, therefore, presents no failure risk. Analysis is similar to that for HGA corrections. This maneuver mode will not be considered further.

A.1.3 RPM Thruster Failures

A recent failure in another satellite thruster system which is based on the Galileo design has caused the Galileo Project to take a careful look at their thruster system. The satellite failed due to operating its thrusters at an operating point which caused thruster overheating and melting, as well as melting of the thermally coupled redundant thrusters. Since the Galileo spacecraft uses thrusters of similar design, an analysis was done to assure that similar failures were not a threat to Earth avoidance or the mission.

The Galileo thrusters are fired at an operating point defined by the flow rate and mixture ratio. Both of these parameters are controlled by adjusting orifice sizes in the RPM design. Figure A-3 shows a plot of possible Galileo operating points. Points to the left of the curves represent points determined through testing to be safe from thermal runaway. The region to the right of the curves is a region where thrusters may overheat and cause destruction of the thruster system. The failed satellite was built without the benefit of such an analysis. Its failure is attributed to operating in the unsafe region in the steady-state mode. That satellite is now operating in the pulsed mode as is its recently launched replacement.

The thruster manufacturer states that the Galileo thrusters are safe if operated at a flow rate of 3.5 gm/s or less. The Galileo system is to be operated at 3.2 gm/s, which provides a safe margin at the expense of thrust level. Adequate testing of thrusters operating at 3.2 gm/s will be performed to guarantee safe operation in pulsed mode.

The remaining concern is the operation of the thrusters in continuous burn mode. The S (spin) and Z (axial) thrusters are used in this mode to change the spacecraft spin rate from 3.15 rpm to 10 rpm and back and to perform large ΔV maneuvers in a turn-burn-turn mode. Testing of thruster operation in continuous burn mode is still in progress to determine that there is no overheating concern and to verify the manufacturer's claim of safe operation at 3.5 gm/s. Furthermore, a fault protection system is being installed on the S and Z thrusters to detect any overheating and to shut them off before redundant thrusters can be affected. This fault protection system consists of redundant temperature sensors on each S and Z thruster and fault protection software. The software will detect thermal runaway and shut down the thruster system within a few seconds, which is adequate to prevent damage to redundant thrusters. The spacecraft will not be operated in continuous burn mode until this fault protection system is in place.

Table A-9. SPIN CORR Probability of Failure due to Stuck Thruster at EGA1 and Resulting in the Following ΔV During the Following Mission Phases

		0.7 m/s	0.4 m/s
VENUS → EGA1 - 25			
AXIAL + Z	$0° < \theta < 30°$	3126×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	3126×10^{-6}	4995×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

EGA1 - 25 → EGA1 -5			
AXIAL + Z	$0° < \theta < 30°$	227×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	227×10^{-6}	363×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4} (EGA1 - 25 to EGA1 -10)
5×10^{-3} (EGA1 - 10 to EGA1 -5)

EGA1 - 5 → EGA1			
AXIAL + Z	$0° < \theta < 30°$	57×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	57×10^{-6}	91×10^{-6}

PROBABILITY OF NO RECOVERY = 10^{-1}

Table A-10. SPIN CORR Probability of Failure due to Stuck Thruster at EGA2 and Resulting in the Following ΔV During the Following Mission Phases

		0.07 m/s	0.4 m/s
APHELION → EGA2 - 25			
AXIAL+ Z	$0° < \theta < 30°$	3808×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	3808×10^{-6}	6085×10^{-6}

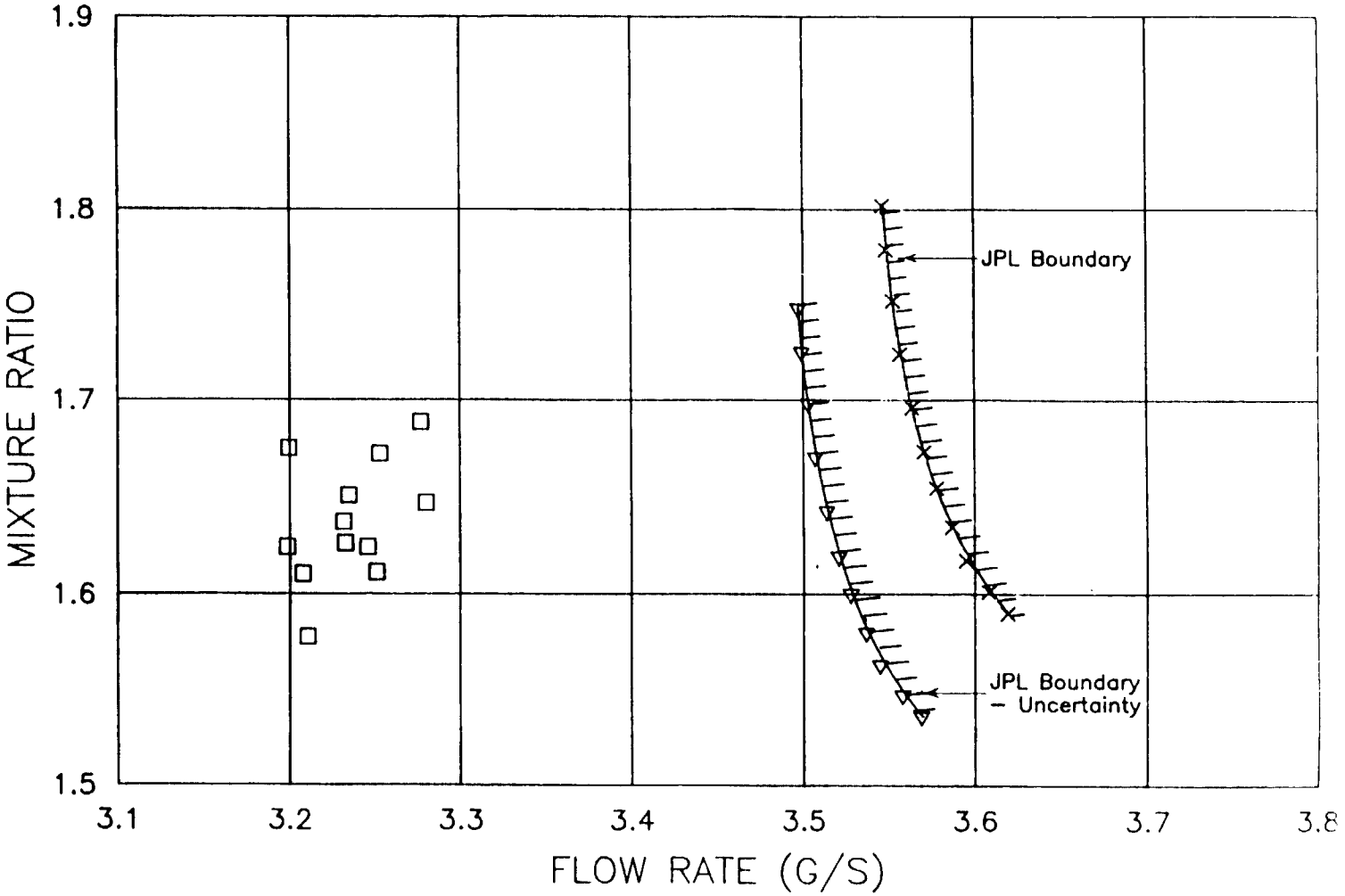
PROBABILITY OF NO RECOVERY = 2×10^{-6}

EGA2 - 25 → EGA2 -5			
AXIAL + Z	$0° < \theta < 30°$	227×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	227×10^{-6}	363×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4} (EGA2 - 25 to EGA2 - 10)
5×10^{-3} (EGA2 - 10 to EGA2 - 5)

EGA2 - 5 → EGA - 2			
AXIAL + Z	$0° < \theta < 30°$	57×10^{-6}	
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$		
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$	57×10^{-6}	91×10^{-6}

PROBABILITY OF NO RECOVERY = 10^{-1}



(Each square corresponds to one of the twelve 10 N thrusters)

Figure A-3. Nominal 10 N Thruster Operating Points (After Adding Bore Hole Orifices)

Thruster overheating does not provide a threat to Earth avoidance with this strategy for thruster operating point verification and fault protection implementation. First, pulsed mode thruster operation cannot lead to thruster overheating, since there is adequate cooling time between pulses. Second, continuous burn mode thruster operation will not be used until fault protection has been implemented to protect the redundant thrusters. The only planned uses of the continuous burn mode before the second Earth flyby are three relatively large maneuvers performed approximately 210 days before the first Earth encounter, before the first asteroid encounter, and at least 100 days before the second Earth encounter. These burns will not be performed in continuous burn mode unless it is determined to be highly unlikely to have a thermal failure. However, even if such a failure occurred, the thruster would be shut down within seconds by a redundant fault protection system. Until time of shutdown, the thruster efficiency would be reduced and the worst effect could be a small thrust for a few seconds in the wrong direction, with a worst-case ΔV error of 0.04 m/s. Since the trajectory never passes close enough to Earth for a ΔV of this size to lead to an impacting trajectory, either while in cruise or during the course of a maneuver, this small erroneous thrust cannot result in an impacting trajectory. Even if it could, the fault protection system would guarantee the integrity of the redundant thrusters. Recovery to a non-impacting trajectory would be highly probable since there are at least 100 days to perform the recovery.

In summary, continuous burn thruster operation is still under investigation, but adequate protection has been implemented to remove any threat to Earth avoidance.

A.1.4 Memory Failure

The failure category under discussion here is one where spacecraft electronics, most likely an AACS memory chip, fails, causing an anomalous thruster firing.

The worst-case situation is a failed AACS memory chip that escapes detection until causing trouble during a TCM. Most AACS memory is checksummed (including all the code) and checksum region failures will be detected almost immediately, although the spacecraft takes no action other than setting an indicator in telemetry. Two failure classes will be examined:

1) A failure that occurs outside of the checksum region such that there is no internal detection,

2) A failure that occurs in the checksum region but within two days of a TCM such that there is insufficient time for detection and corrective action from the ground.

Failure Occurs Outside Checksum. The probability that an AACS memory chip fails during the mission has been calculated from the upper limits of TCC244 memory chip failure rates obtained by testing.

P(an AACS memory chip fails during mission) = 0.4

All but 5376 of 32768 bytes of memory are checksummed.

P(occurs outside checksum region) = 5376/32768 = 0.16

To cause impact, a burn must be either too big or in the wrong direction, or both. If a failed chip led to a burn too big, it would be terminated by the backup 7STOP command which is built into all maneuver sequences. However, if data storage related to stator orientation were affected, then a lateral burn could occur in the wrong direction anywhere in the plane perpendicular to the axial without on-board detection. Data used to control stator orientation, and which are outside of the checksum region, are stored in scan data (60 locations).

P(failure occurs in scan data) = 60/5376 = 0.011

Most locations in scan data are also used by the HGA correct algorithm, so that failure of this algorithm would provide early detection.

P(not detected by HGA cor) = 0.1

Then the probability per year of a failed memory chip which could lead to an anomalous thrust without detection is:

P(occurs undetected per year) = 0.4/8*0.16*0.011*0.1 = 9.E-6

The probability of a memory chip failure outside of the checksum region which causes a velocity error (DVL) is given below. The failure causes the intended lateral burn velocity magnitude (V_{lat}) to be delivered, but in the wrong direction. The period of vulnerability is the time elapsed since the last maneuver.

Venus to EGA1-60:	P = 9.E-6*240/365 = 5.7E-6	DVL = V_{lat}
EGA1-60 to EGA1-25:	P = 9.E-6*35/365 = 0.8E-6	DVL = V_{lat}
EGA1-25 to EGA1-10:	P = 9.E-6*15/365 = 0.4E-6	DVL = V_{lat}
Aphelion to EGA2-60:	P = 9.E-6*300/365 = 7.2E-6	DVL = V_{lat}
EGA2-60 to EGA2-25:	P = 9.E-6*35/365 = 0.8E-6	DVL = V_{lat}
EGA2-25 to EGA2-10:	P = 9.E-6*15/365 = 0.4E-6	DVL = V_{lat}

Failure Occurs Inside Checksum. The remaining memory is checksummed:

P(occurs inside checksum) = 0.84

This failure could cause damage to code or permanent data. In most cases an error causing improper execution of a TCM would trip fault protection, but commanding the wrong thruster to fire might not be detected by plume impingement fault protection. This could result in delivering the intended velocity magnitude, but in the wrong direction. Such errors would be concentrated in the turnburn or burngo algorithms which occupy about 4% of the checksum region.

P(occurs in turnburn or burngo) = 0.04

Assuming that it is not possible to detect and respond to a checksum error arising within the two days preceding a TCM, the probability of this failure occurring per two days is:

$$P = 0.4/8*0.84*0.04*2/365 = 9.2E-6$$

Let the intended TCM velocity be V_{nom}. The velocity error (DVL or DVZ) may be lateral or axial with equal probability. Then for each burn type (LAT, POSZ, PULZ, NEGZ) in the TCMs preceding EGA1 or EGA2:

$P = 4.6\ E-6 \quad DVL = V_{nom}$
$P = 4.6\ E-6 \quad DVZ = V_{nom}$

Failure probabilities are summarized in Table A-11.

A.1.5 Structural Failures

Beyond the obvious requirement to keep the spacecraft together, Galileo's structure plays a vital role in stabilizing the spacecraft. Galileo, like all spinning spacecraft, must have proper ballasting, structural alignments, and control of mass properties to remain dynamically stable. If, for example, an improperly designed piece of structure broke and released a large component, the resulting shift in mass properties would affect the spacecraft's rotation. At best, the spacecraft would be left with an uncorrectable wobble which would degrade telecommunications and science instrument pointing. At worst, the resulting nutation and wobble may make the spacecraft uncontrollable.

Given the navigation strategy which biases the spacecraft trajectory, even worst-case structural failures which release hardware would have almost no chance of leading to Earth impact. The only hypothesized case where Earth impact could be imagined are failures where an RTG breaks free and flies off on its own trajectory. As will be shown in the following paragraphs, the spacecraft's design makes this scenario implausible.

By themselves, most structural failures produce little or no ΔV and so do not risk Earth impact. In the case of an RTG, if one could break free, and if its angular momentum could hurl it away from the remainder of the spacecraft, it would become uncontrollable and a potential hazard to the Earth.

However, this worst-case scenario is not credible for several reasons. First, all spacecraft structure, including the RTG booms, is designed with a large margin of safety (a factor of 1.4 or greater). Second, prior to launch, the entire spacecraft is exhaustively tested on a dynamic shake table to validate that all structural members can withstand launch vibration, the worst dynamic environment of the entire mission. Finally, even if an RTG boom could completely disintegrate, the RTG would still be retained by heavy electrical cables. These cables can easily hold the RTG even against the tension (about 40 pounds at 10 rpm) resulting from a stuck-open spin thruster (second fault) before onboard fault protection software intervenes. Although a dangling RTG would leave the spacecraft with a severe wobble, the RTG would remain with the spacecraft.

Table A-11. Probability of Failure Due to AACS Memory Chip Failure and Resulting in the Following ΔV During the Following Mission Phases

		$\lvert\Delta V\rvert = \lvert V_{NOM}\rvert$
AT EGA - 60		
AXIAL Z	$0° < \theta < 30°$	2.3×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	*
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	2.3×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

*10.3×10^{-6}	AT EGA1
11.8×10^{-6}	AT EGA2

AT EGA - 25		
AXIAL + Z	$0° < \theta < 30°$	2.3×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	5.4×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	2.3×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA - 10		
AXIAL + Z	$0° < \theta < 30°$	2.3×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	5.0×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	2.3×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4}

Given the design and testing practices which secure the RTG, there is no credible structural failure which could lead to an RTG becoming separated from the spacecraft. Accordingly, the probability of this failure type is treated as zero.

A.1.6 AACS Flight Software Coding Error

The failure mode to be discussed here is one where an AACS flight software programming error causes an anomalous thruster firing. A flight software programming error may affect execution of some maneuver which fires thrusters. The software error may be present at launch, or it may be introduced by an in-flight software code change. A software error present at launch would very likely be detected by TCMs preceding the Venus flyby. It is more likely that such an error near Earth encounter would be introduced by an in-flight software change. No such in-flight software changes are planned until after the second Earth encounter.

Only during a propulsive maneuver, when the isovalves have been opened, can a software error cause an anomalous thruster firing. HGA correction maneuvers will be performed approximately daily. Flight software code errors which affect the HGA correction maneuver would therefore be detected early. In spin correction maneuvers, an anomalous thruster firing would trip fault protection while imparting only a fraction of a meter per second at most. The worst situation is an error affecting vector mode maneuvers and not affecting HGA corrections. If an error caused a burn to be too big, the burn would be stopped by the backup 7STOP command which is built into each burn sequence. However, an error in the burn control algorithm could cause either of the following problems which would escape on-board detection:

1) Lateral burn executed in the wrong direction, anywhere in the plane perpendicular to the axial direction (turnburn algorithm), or

2) Select the wrong thruster (burngo algorithm).

Given the level of testing to which the software is subjected, it is estimated that the probability of discovering in-flight an AACS software coding error is bounded by 0.1 for the eight year mission. In the Voyager mission to date, no such AACS software errors have been encountered during execution.

P(error occurs during mission) = 0.1

The turnburn and burngo algorithms in the AACS constitute about 4% of the flight code, and only about 10% of their code is related to lateral burns or to thruster selection and not used in HGA corrections.

P(occurs in turnburn or burngo) = 0.04
P(affects lat burn or thruster ID, not HGA) = 0.1

The probability density for error occurrence is taken to be uniform in time. Then the probability of error occurrence per year is:

P(occurs per year) = 0.1/8*0.04*0.1 = 50.E-6

An error in the critical section of code may or may not affect the burn results. If the error affects the burn magnitude only, it cannot lead to an impacting trajectory because burns too large are stopped by the backup 7STOP command, and burns too small cannot result in an impacting trajectory. If the error affects the burn arc or thruster selection, a burn of the right magnitude but in the wrong direction may result. A worst-case assumption is used, that the software error has a 50% chance of a resultant burn in the wrong direction.

The probability of a software code error causing an anomalous velocity is found below, where the period of vulnerability is the time elapsed since the last maneuver. Backup 7STOP commands will prevent imparting too much velocity, but the intended velocity magnitude (V_{nom}) may be delivered in the wrong direction. The velocity error (DVL or DVZ) may be lateral or axial with equal probability.

Venus to EGA1-60:	P = 12.5E-6*240/365 =	8.2E-6	DVL = V_{nom}
Venus to EGA1-60:	P = "	8.2E-6	DVZ = V_{nom}
EGA1-60 to EGA1-25:	P = 12.5E-6*35/365 =	1.2E-6	DVL = V_{nom}
EGA1-60 to EGA1-25:	P = "	1.2E-6	DVZ = V_{nom}
EGA1-25 to EGA1-10:	P = 12.5.E-6*15/365 =	0.51E-6	DVL = V_{nom}
EGA1-25 to EGA1-10:	P = "	0.51E-6	DVZ = V_{nom}
Aphelion to EGA2-60:	P = 12.5E-6*300/365 =	10.0E-6	DVL = V_{nom}
Aphelion to EGA2-60:	P = "	10.0E-6	DVZ = V_{nom}
EGA2-60 to EGA2-25:	P = 12.5E-6*35/365 =	1.2E-6	DVL = V_{nom}
EGA2-60 to EGA2-25:	P = "	1.2E-6	DVZ = V_{nom}
EGA2-25 to EGA2-10:	P = 12.5E-6*15/365 =	0.51E-6	DVL = V_{nom}
EGA2-25 to EGA2-10:	P = "	0.51E-6	DVZ = V_{nom}

Failure probabilities are summarized in Tables A-12 and A-13.

A.1.7 CDS Software Errors

The failure mode considered here is one where commands correctly received by the CDS are subsequently transferred to other subsystems erroneously, causing spacecraft events which result in an anomalous velocity increment. The most likely specific failure in this category is one where the CDS sends an erroneous command to AACS. To be accepted by AACS, the command must have a correct checksum. In the worst case, the command causes the AACS to execute an anomalous burn.

The CDS is designed such that there is no more than a 1% chance of sending an anomalous command to the AACS during the mission. The probability of this command occurring in the 34 months between Venus closest approach and EGA 2 is:

$$0.01 \times (34 \text{ months} / 8 \text{ years}) = 3.5 \times 10^{-3}.$$

Table A-12. Probability of Failure Due to AACS Programming Error at EGA1 and Resulting in the Following ΔV During the Following Mission Phases

		$\lvert\Delta V\rvert = \lvert V_{NOM}\rvert$
AT EGA1 - 60		
AXIAL + Z	$0° < \theta < 30°$	4.1×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	8.2×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	4.1×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA1 - 25		
AXIAL +Z	$0° < \theta < 30°$	0.6×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1.2×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	0.6×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA1 - 10		
AXIAL + Z	$0° < \theta < 30°$	0.26×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	0.51×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	0.26×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4}

Table A-13. Probability of Failure Due to AACS Programming Error at EGA2 and Resulting in the Following ΔV During the Following Mission Phases

		$\lvert\Delta V\rvert = \lvert V_{NOM}\rvert$
AT EGA2 - 60		
AXIAL+Z	$0° < \theta < 30°$	5.0×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	10.0×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	5.0×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA2 - 25		
AXIAL+Z	$0° < \theta < 30°$	0.6×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1.2×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	0.6×10^{-6}

PROBABILITY OF NO RECOVERY = 2×10^{-6}

AT EGA2 - 10		
AXIAL+ Z	$0° < \theta < 30°$	0.26×10^{-6}
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	0.51×10^{-6}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	0.26×10^{-6}

PROBABILITY OF NO RECOVERY = 3×10^{-4}

A sixteen-bit checksum is attached to every AACS command in order to prevent such anomalous commands from affecting the spacecraft. Accidentally getting this checksum correct has a probability of

$$2\text{-}16 = 1.5 \times 10^{-5}$$

The most likely way for such a command to be received by the AACS is for a valid command to be anomalously distorted into an AACS command which induces thruster action and for that command to have the checksum just happen to be correct. The probability for this occurring between Venus CA and EGA2 is

$$(3.5 \times 10^{-3}) \times (1.5 \times 10^{-5}) = 5 \times 10^{-8}$$

For the following specific periods, probabilities are:

EGA 1 -60 days to EGA 1 -25 days: 1.7×10^{-9}
EGA 1 -25 days to EGA 1 -5 days: 9.8×10^{-10}
EGA 1 -5 days to EGA 1: 2.5×10^{-10}
EGA 2 -60 days to EGA 2 -25 days: 1.7×10^{-9}
EGA 2 -25 days to EGA 2 -5 days: 9.8×10^{-10}
EGA 2 -5 days to EGA 2: 2.5×10^{-10}

It should be noted that these probabilities only account for an erroneous command being sent by the CDS, and then being accepted by the AACS, with no allowance for the further reduction when considering the likelihood that such a command would lead to a thruster firing. This factor was not pursued in this analysis, since the probabilities are already so small as to present no risk to Earth impact.

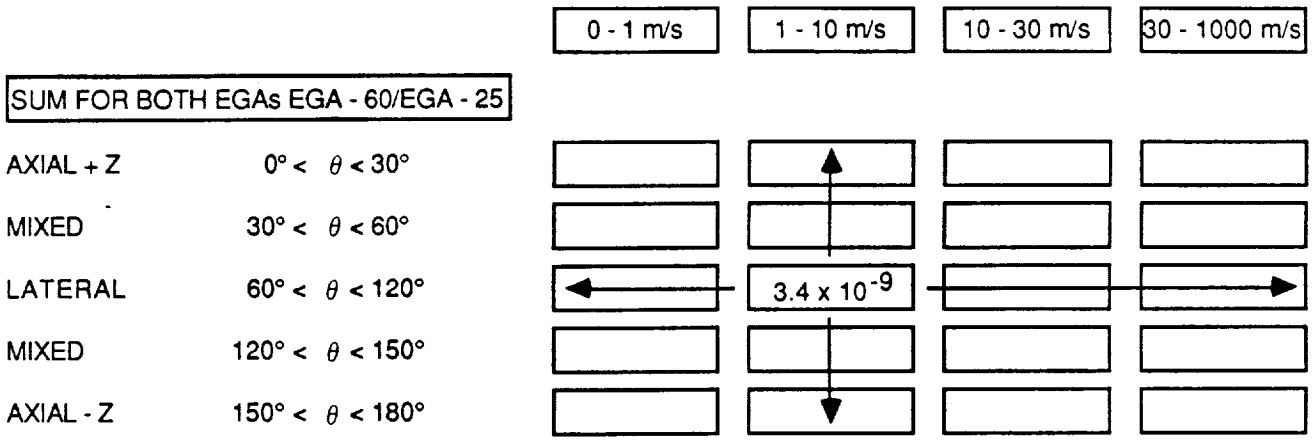
The probability of recovery from such a failure depends upon the time available before the next Earth encounter. Recovery probabilities have been taken from Section 3.2.3 since the initial failure in this case does not interfere with recovery. The failure probabilities for this category are shown in Table A-14.

A.1.8 Spacecraft Drifts Off Sunline

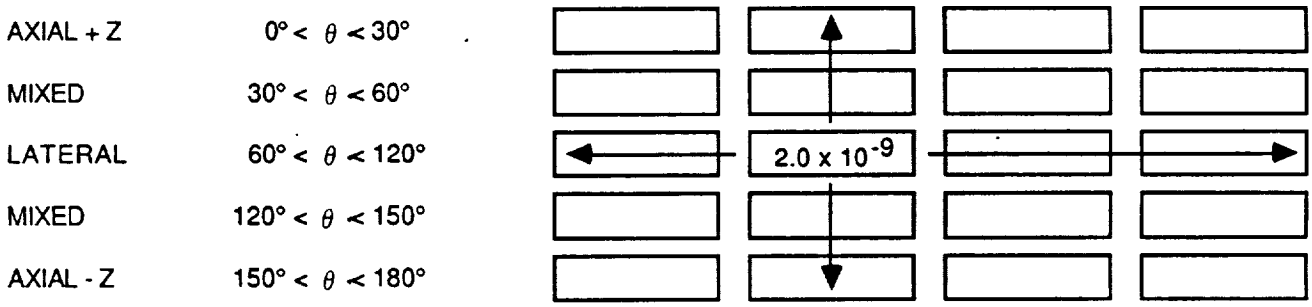
The Galileo spacecraft is protected from extreme temperature excursions by multi-layer insulation (MLI), which envelopes critical subsystems (including the four Retro Propulsion Module (RPM) propellant tanks), and by mechanical and structural shade devices. The thermal control systems are designed such that subsystem temperatures will remain within flight allowable limits as long as the angle between the spacecraft's -Z-axis and the Sun remains less than 14°. If the spacecraft loses its Sunpoint during the first three years of its mission, the resulting thermal problems could lead to failures which could cause a ΔV, either through inadvertent thruster firings or through an impulse due to RPM tank rupture.

Several thermally induced failures were examined, but only two were determined to be serious enough to analyze in detail. Electronic parts failures due to high temperatures resulting from offsun conditions are shown to have very low probabilities of causing ΔVs. RPM tank rupture due to thermally induced overpressure was originally shown to be of significant concern; however, as a consequence of this determination, the Galileo Project

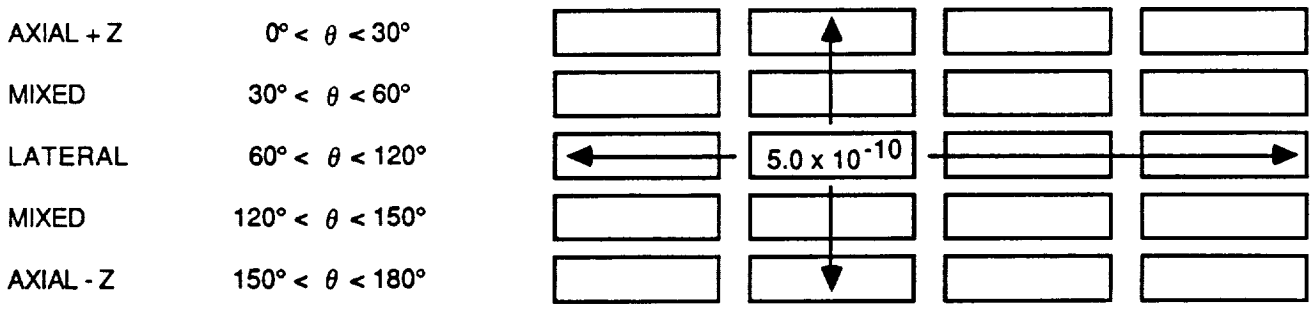
Table A-14. Probability of Failure due to CDS Software Failure and Resulting in the Following ΔV During the Following Mission Phases



PROBABILITY OF NO RECOVERY = 2×10^{-6}



PROBABILITY OF NO RECOVERY = 3×10^{-4} (EGA - 25 to EGA -10)
5×10^{-3} (EGA - 10 to EGA -5)



PROBABILITY OF NO RECOVERY = 10^{-1}

has incorporated changes to the RPM design which will prevent RPM tank rupture due to overpressure. The spacecraft would lose attitude control capability if both redundant halves of some element in the command chain failed. This could occur in the RFS, MDS, CDS, or AACS.

A.1.8.1 RPM Tank Rupture. One of the most important variables for a meaningful analysis of thermal failure modes is the process of heating the RPM tanks. For the purposes of this analysis, worst case conditions were used to evaluate the probability of RPM tank rupture. Heat transfer from the RPM tanks to cooler portions of the spacecraft (e.g., the bus) was intentionally minimized. No blocking effects on direct solar heating of the tanks were incorporated into this analysis. This is conservative since in reality the spacecraft structure will shade much of the RPM subsystem even when offsun. The outer layer (black Kapton) of the blankets does not degrade or disappear even at the worst case (non-spinning near Venus) temperature of 240°C. This is conservative since loss of the polyester binder in the blankets' carbon would result in lower solar absorptance (i.e., lower tank temperatures).

In addition, this study limited its analysis to the spacecraft spinning condition (non-spinning cases were evaluated, but determined to be very improbable because it takes a precise attitude control adjustment to completely nullify the spacecraft's rotational velocity). The outer blanket surface reaches an average temperature around its circumference based on the thermal equilibrium induced by the spinning condition. The heating sources on the outer blanket surface consist primarily of direct solar heating and to a lesser extent heat dissipated from the shunt heater. The shunt heater converts the excess electrical power of the spacecraft electronic subsystems to heat which is radiated to the RPM tanks, then ultimately through the blankets to space. For this study, two shunt heater power states were considered: the nominal power of 49 W and an unpowered case. (If the spacecraft is pointed offsun, potential subsystem overtemperature failures could reduce the amount of electrical power consumed by the subsystems and thus increase the amount of heat dissipated by the shunt heater. Over 75 W of power could be reasonably expected under these conditions. Although these cases were not analyzed in detail, the RPM design changes that have been incorporated into the spacecraft will eliminate these cases as concerns.)

The distance of the spacecraft from the Sun and the angular velocity of the spacecraft relative to the Sun as functions of mission time were accurately modelled in the analysis. The maximum allowable tank temperatures (burst temperatures) as a function of time (Figure A-4) were derived from a detailed analysis of tank stress tolerance as a function of temperature and tank ullage.

The determination of the probability of tank rupture begins with the determination of the probability of loss of both strings of a subsystem critical to communication and control. Any such loss requires at least a two point failure. A two point failure in a specified system has a probability of 10^{-4} of occurring sometime during the mission (see Sections 3.2.1 and 3.2.2). There are three potential failure locations within the CDS: HCD, HLM, and Bus; three potential failure locations within the AACS: CPU, IO, and PDE; one potential failure location in the RFS, and one potential failure location in the MDS. This results in a total probability of 8×10^{-4} for a two point failure causing the loss of a critical communication subsystem.

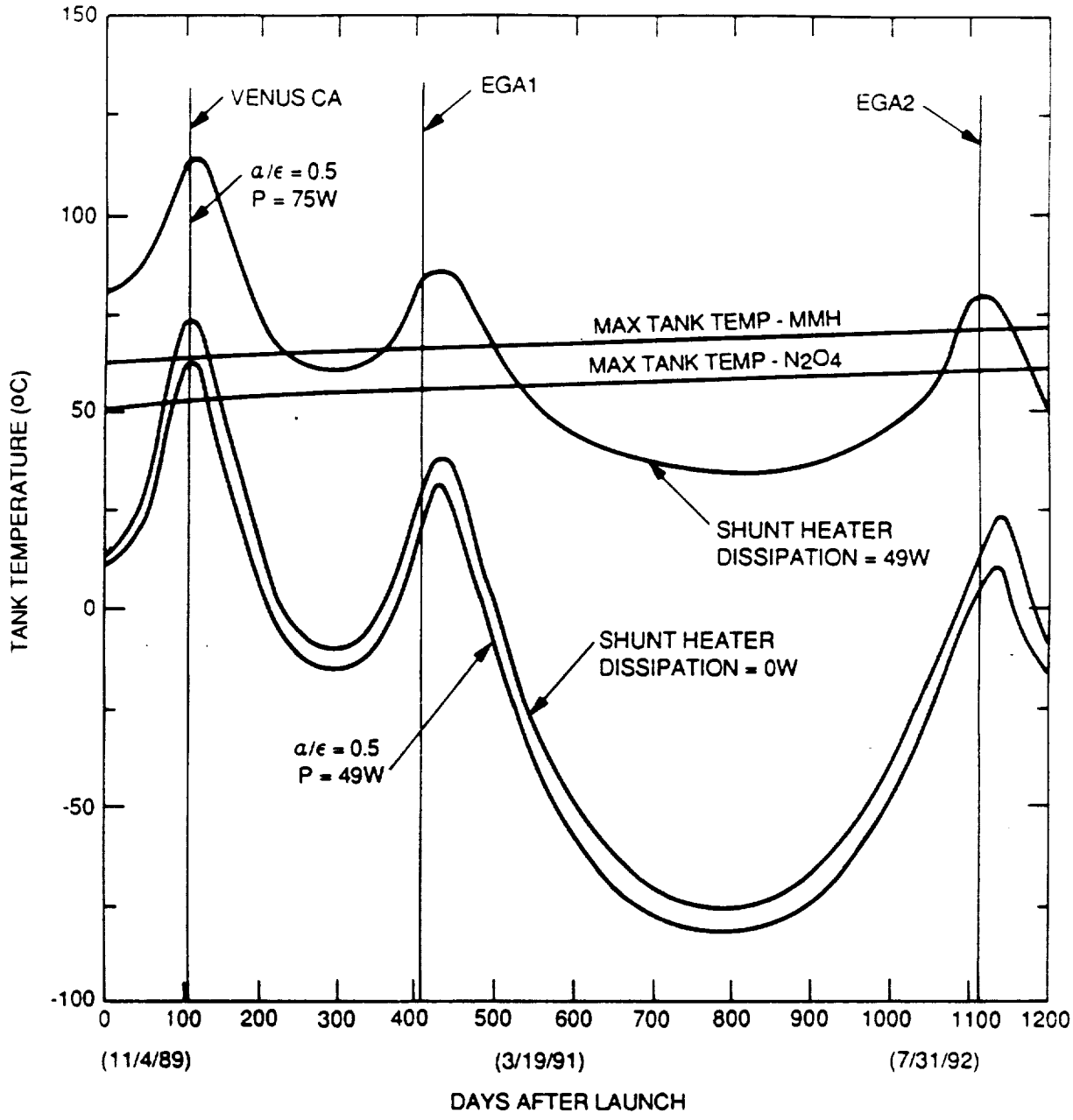


Figure A-4. Steady-State Tank Temperatures for 90° Off-Sun Attitude

The determination of the probability of tank rupture continues with the determination of the probability of the tanks exceeding their burst temperature. Examples of typical tank temperature histories during offsun conditions for loss of command capability at 250, 550, and 800 days are shown in Figures A-5 and A-6. Note that loss of command capability at 250 days results in tank burst at about 370 days, very close to the first Earth encounter. Loss of command capability at 550 days is not a problem since the tank burst temperature is reached after the second Earth encounter. However, loss of command capability at 800 days results in at 800 days results in tank burst temperatures being exceeded just a few days before the second Earth encounter.

The length of time from loss of command capability to tank burst is obtained by determining when the tank temperature will exceed its limit. This is done for each day of the mission. This information is plotted on Figure A-7 for launch through the second encounter. There are three periods of vulnerability where the time of tank burst following loss of command capability is before one of the two encounters.

The first period of vulnerability is from Venus CA-30 (closest approach minus 30 days) to EGA1-90, resulting in tank burst prior to EGA1. (The period begins at Venus CA-30 rather than launch because this is the first time when the actual rupture would occur after Venus CA. A rupture before Venus CA is extremely unlikely to result in an impacting trajectory.) This is eight percent of the mission (240 days/8 years). The total probability of the tanks bursting during the first period of vulnerability is thus 6.4×10^{-5} ($0.08 \times 8 \times 10^{-4}$). The time of the tank rupture due to a loss of command capability in this period ranges from Venus CA to EGA1.

The second period of vulnerability is from EGA1-90 to EGA1+75, resulting in tank burst after EGA1 but prior to EGA2. This is six percent of the mission (165 days/8 years). The total probability of the tanks bursting during the second period of vulnerability is thus 4.8×10^{-5} ($0.06 \times 8 \times 10^{-4}$). The time of tank rupture due to a loss of command capability in this period ranges from EGA1 to EGA2, but is strongly weighted toward the first 100 days after EGA1. Note that a rupture during the first 100 days after EGA1 is unlikely to result in an impacting trajectory since there would be no opportunity for the necessary trajectory correction maneuver to target the spacecraft for EGA2. This second period of vulnerability is thus broken into two subperiods, EGA1-90 to EGA1+50 when the rupture occurs during the first 100 days after EGA1, and EGA1+50 to EGA1+75 when the rupture occurs closer to EGA2. The probabilities of burst for these two subperiods are 4.1×10^{-5} and 7.3×10^{-6}, respectively.

The third period of vulnerability is from EGA2-345 to EGA2-145, resulting in tank burst very near EGA2. This is seven percent of the mission (200 days/8 years). The total probability of the tanks bursting during the third period of vulnerability is thus 5.6×10^{-5} ($0.07 \times 8 \times 10^{-4}$). For this third period, the rupture will occur between EGA2-10 and EGA2.

Note that the periods of EGA1+75 to EGA2-345 and EGA2- 145 and beyond all result in tank burst after EGA2 and therefore are of no concern with regard to the Earth avoidance issue.

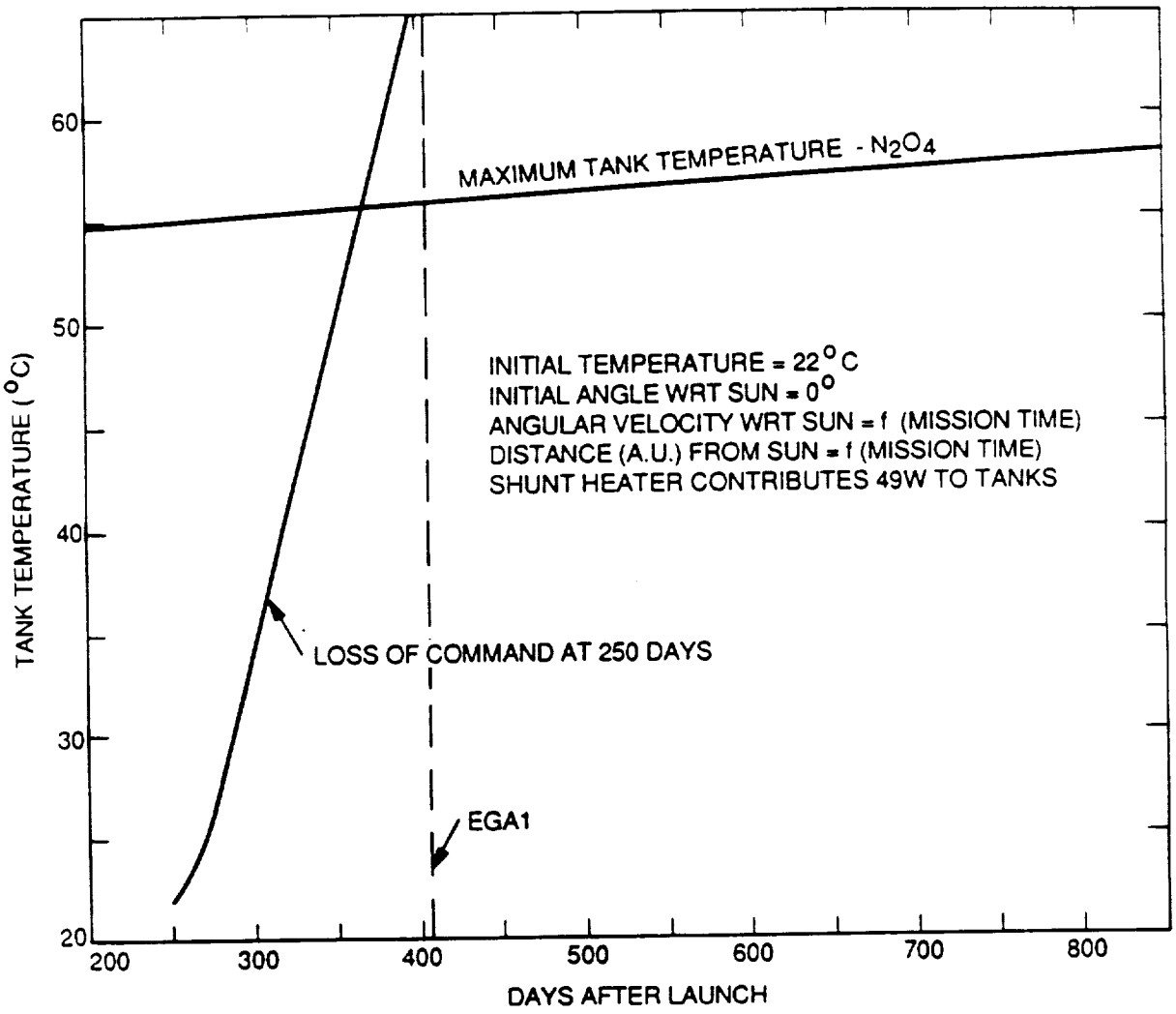


Figure A-5. Galileo RPM Tank Temperature During Off-Sun Conditions at EGA1

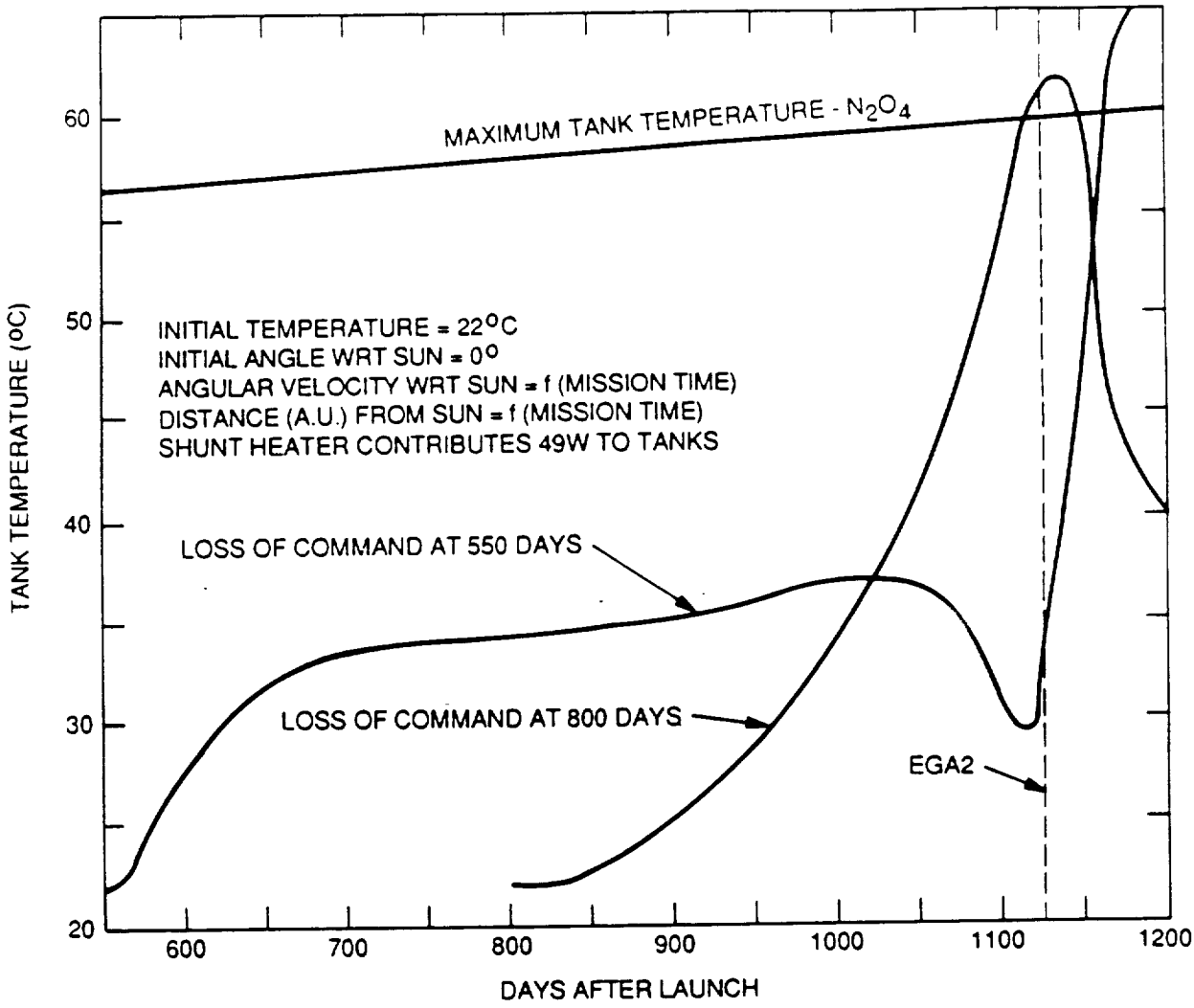


Figure A-6. Galileo RPM Tank Temperature During Off-Sun Conditions at EGA2

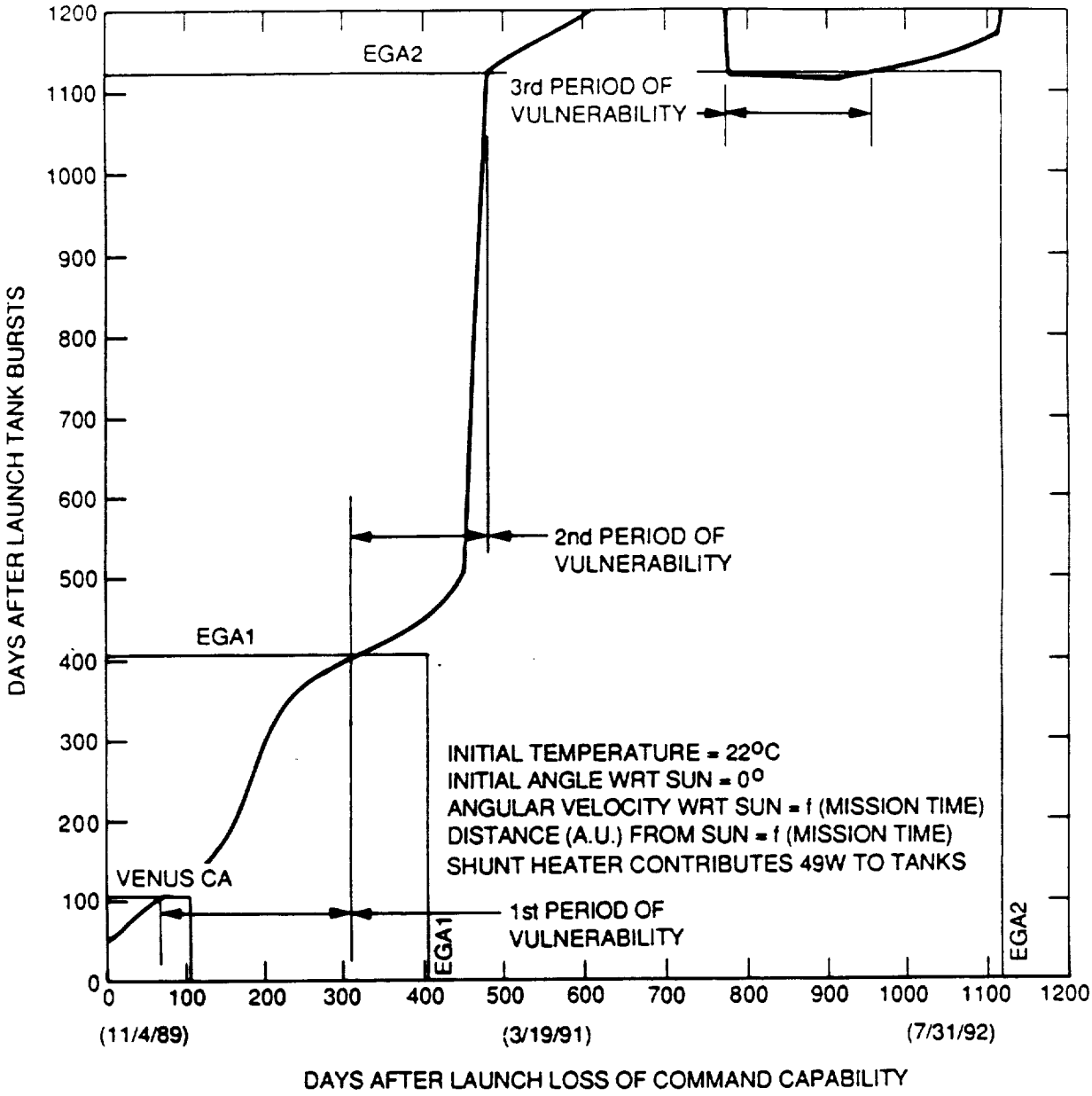


Figure A-7. Time of OX Tank Burst After Time of Command Loss

In all of the periods, the worst case failure mode of the tanks was determined to be a sudden rupture as opposed to a leak since the tanks will be stressed to the point of failure of the tank wall. The ΔV imparted to the spacecraft due to the escaping liquid in the ruptured tank is a function of the ullage in the tank at the time of rupture. The rupture was modelled for each type of tank and for each period of vulnerability. It was determined that one nitrogen tetroxide tank would rupture first, imparting a ΔV to the spacecraft. This would relieve the pressure on the remaining nitrogen tetroxide tank, and escaping liquid and gas from it would have an additional effect on the spacecraft velocity. This event would be followed by a similar rupture of one mono-methyl hydrazine tank imparting another ΔV and relieving the remaining tank. The resulting ΔV would be the vector sum of the effects of the two tank ruptures.

Several hardware changes were considered to reduce the offsun risk to the RPM tank. The two most viable changes were to add a pressure relief system to the oxidizer and fuel tanks and to put new insulation blankets with a low absorptance to emittance ratio around the RPM tanks. Due to its superior results in reducing the offsun risk to the RPM tanks (as well as protecting against high shunt heater power dissipation), a pressure relief system was chosen to be incorporated into the spacecraft (ref. JPL IOM 353-GLL-88-007, R. Fradet to R. Spehalski, "Conceptual Design of a Relief System to Protect Against RPM Thermal Overpressure;" January 25, 1988).

The pressure relief system (shown in Figure A-8) consists of a burst disk/relief valve provided to each of the oxidizer and fuel tank pressurization systems down stream of the check valves. Each vent line is terminated with a T to insure that no net ΔV is caused by venting of helium and propellant vapors.

This design change was readily incorporated into the RPM with minimal packaging impact, and did not have any impact on any shuttle safety items. The long exposure time of the burst disk to propellant vapors is a potential mission reliability concern, but the Viking 75 mission provided successful in-flight experience with identical hardware. However, if the effectiveness of the burst disk is degraded, the relief valve will continue to provide adequate, albeit with loss of redundancy, overpressurization protection.

This design concept will reduce the probability of RPM tank rupture by 10^{-4}, the chance that the redundant pressure relief valve system fails to operate. Thus, the worst case probability of tank rupture is the sum of the probabilities from each period of vulnerability from above multiplied by 10^{-4}, i.e., $(6.4 \times 10^{-5} + 4.1 \times 10^{-5} + 7.3 \times 10^{-6} + 5.6 \times 10^{-5}) \times 10^{-4}$ which equals 1.7×10^{-8}.

A.1.8.2 Electronics (AACS) Parts Failure. Several worst case conditions were used to evaluate the probability of electronic parts failure. The most conservative VEEGA Mission Bay 8 shear plate prediction (33°C) was used for this study. A simple equilibrium energy balance between the Bay 8 shear plate and the AACS, which included solar heating of the AACS, was used to calculate AACS piece part temperatures for both spinning and non-spinning conditions. For these failures, only conservative steady-state conditions with the spacecraft's Z-axis perpendicular to the Sun were considered. The energy

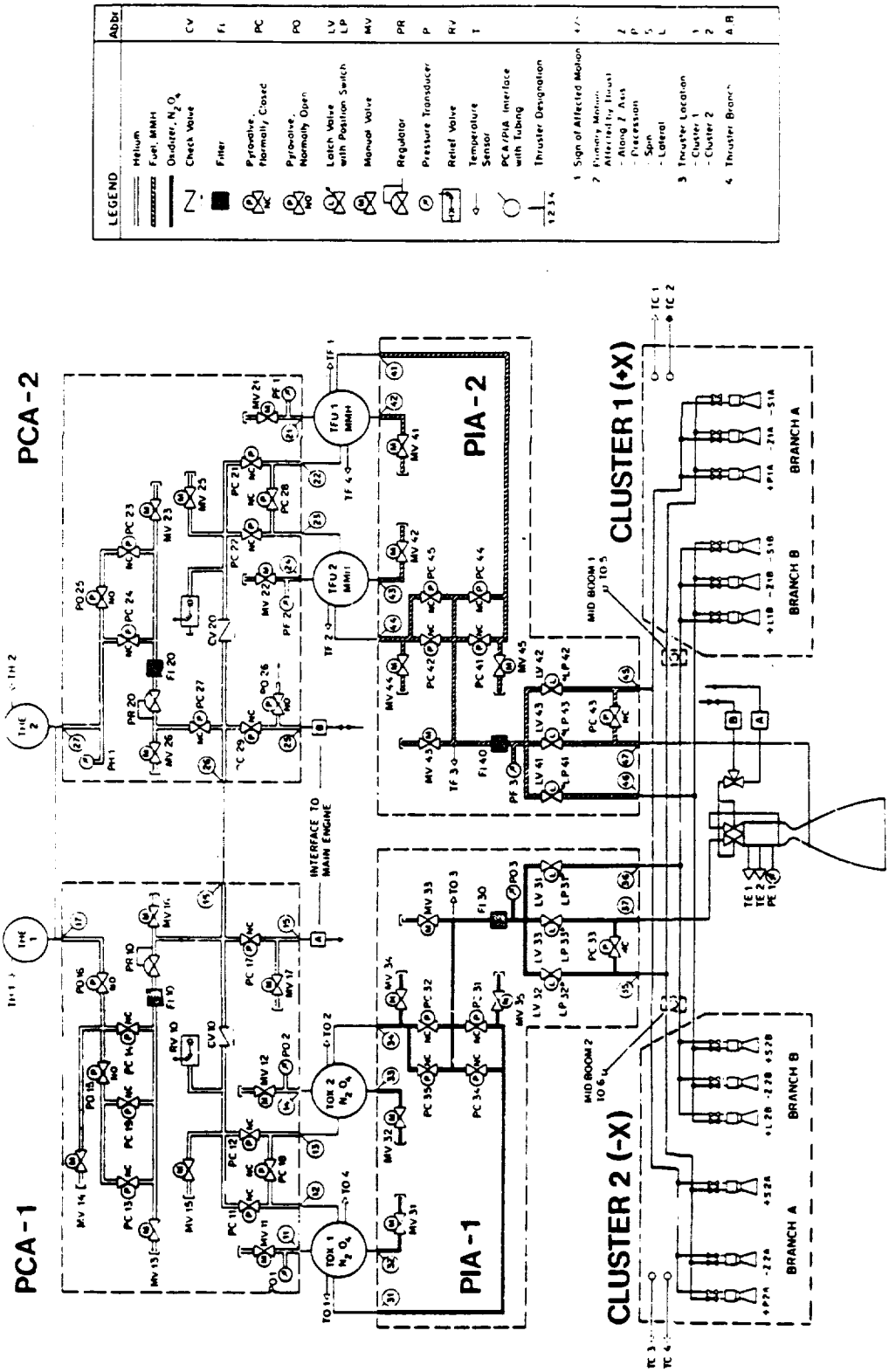


Figure A-8. Galileo Retro Propulsion Module (RPM) Schematic

balance used values of absorptance and emittance equal to 0.32 and 0.8, respectively, for the louver system on the AACS. To be conservative, a 30°C rise from the shear plate to the junction was used. Generic IC single piece part failure probabilities were calculated from MIL-STD-217E. The probability of failure of electronic piece parts equals 1.0 when their junction temperature reaches 175°C. Figure A-9 shows the AACS part temperatures for a 90° off-Sun attitude for both spinning and non-spinning bus cases. Figure A-10 shows the probability of failure for various AACS logic devices at a spinning 90° off-Sun attitude.

The determination of the probability of electronic parts failure begins with the determination of the probability of an occurrence which leads to an offsun condition. Any such occurrence must be the result of a two point failure which has been previously shown to have a probability of 8×10^{-4}. The determination of the probability of electronics parts failure continues with the determination of the probability of a PDE parts failure which leads to thrust. A very conservative upper bound for the number of parts for which a failure may affect the thrust valves is 103. If the parts are 90° offsun for 10 days near Venus CA (the worst case) then the probability of a single part failure is 0.015 (0.06/106 hours x 10 days x 103 parts). The probability of a part failure at some time in the mission affecting thruster valves is not greater than 1.2×10^{-5} ($0.015 \times 8 \times 10^{-4}$). Since these probabilities are very small, upper bounds for this category can be calculated.

If the probability of a parts failure is equally likely from Venus CA to EGA2 (assumed to be the worst-case value of 0.06×10^{-6} failures per hour from Figure A-10), then the probability of failure from EGA-180 to EGA-20 is 6.6×10^{-7} (160 days/8 years x 1.2×10^{-5}), the probability from EGA-20 to EGA-10 is 4.1×10^{-8} (10 days/8 years x 1.2×10^{-5}), the probability from EGA10 to EGA-3-1/2 is 2.7×10^{-8} (6-1/2 days/8 years x 1.2×10^{-5}), the probability from EGA-3-1/2 to EGA-1 is 1.0×10^{-8} (2-1/2 days/8 years x 1.2×10^{-5}), and the probability from EGA-1 to EGA is 4.1×10^{-9} (1 day/8 years x 1.2×10^{-5}). These values are applicable to both EGA1 and EGA2.

A.1.8.3 Other Failures. Other failures involving an offsun condition were considered, but are not worst case scenarios. For example, thruster valve failure due to drifting offsun is not probable because valves are acceptance tested to 115°C and are designed to survive to 160°C, but the valves' temperatures will always be less than or equal to the tanks' temperatures which will never exceed 114°C as shown by analysis (Figure A-4). Another example, stuck thrusters, is not a worst-case cause of drifting off-Sun because although stuck thrusters are caused by a two point failure and they result in an unpredictable offsun condition followed by orbital drift, they have a very high probability of recovery unlike the communication failure which assumes none.

The probabilities of RPM tank rupture as a function of mission time and resulting ΔVs are shown in Table A-15.The probabilities of electronics (AACS) parts failure are shown in Table A-16.

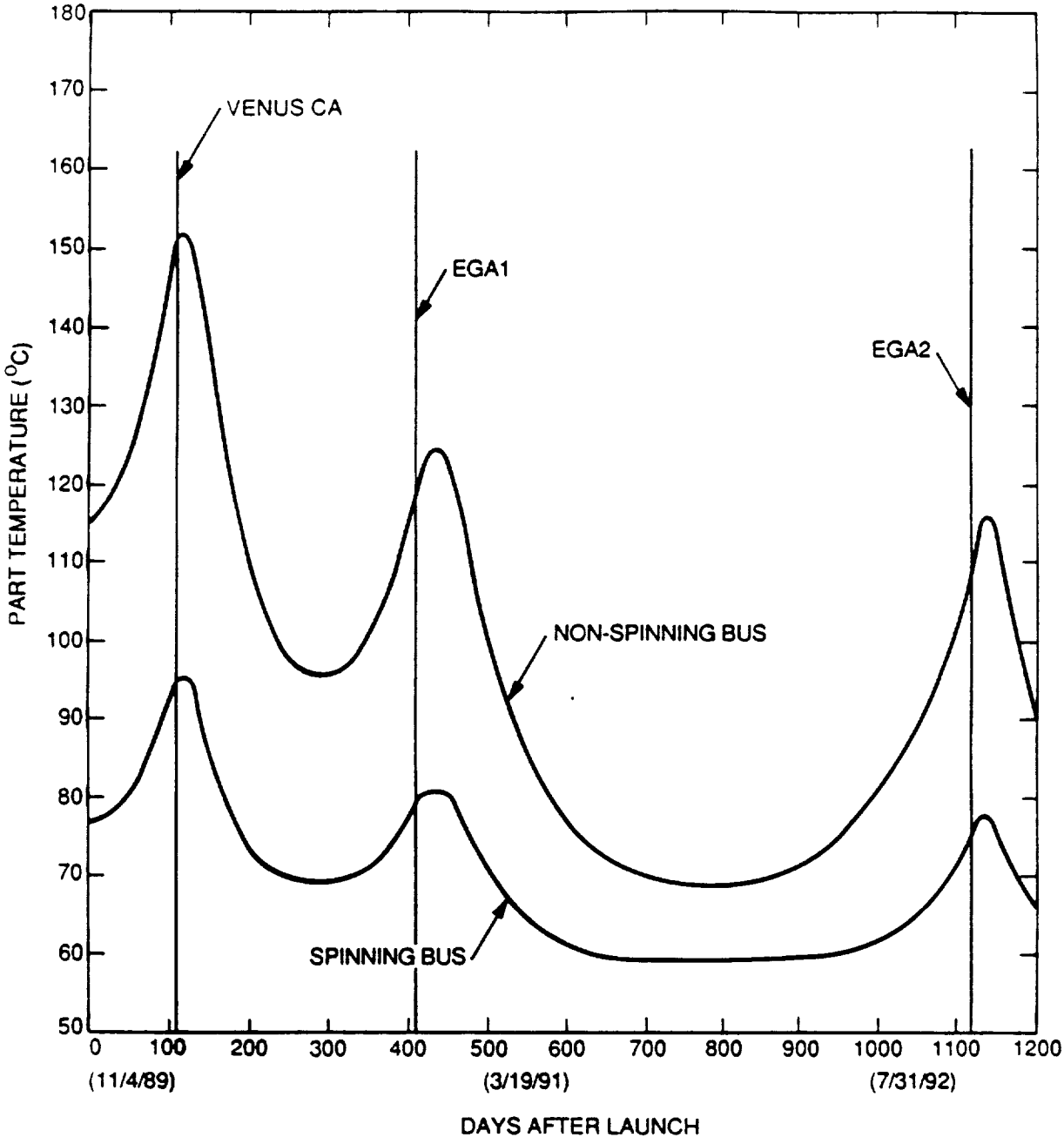


Figure A-9. AACS Part Temperatures for 90° Off-Sun Attitude

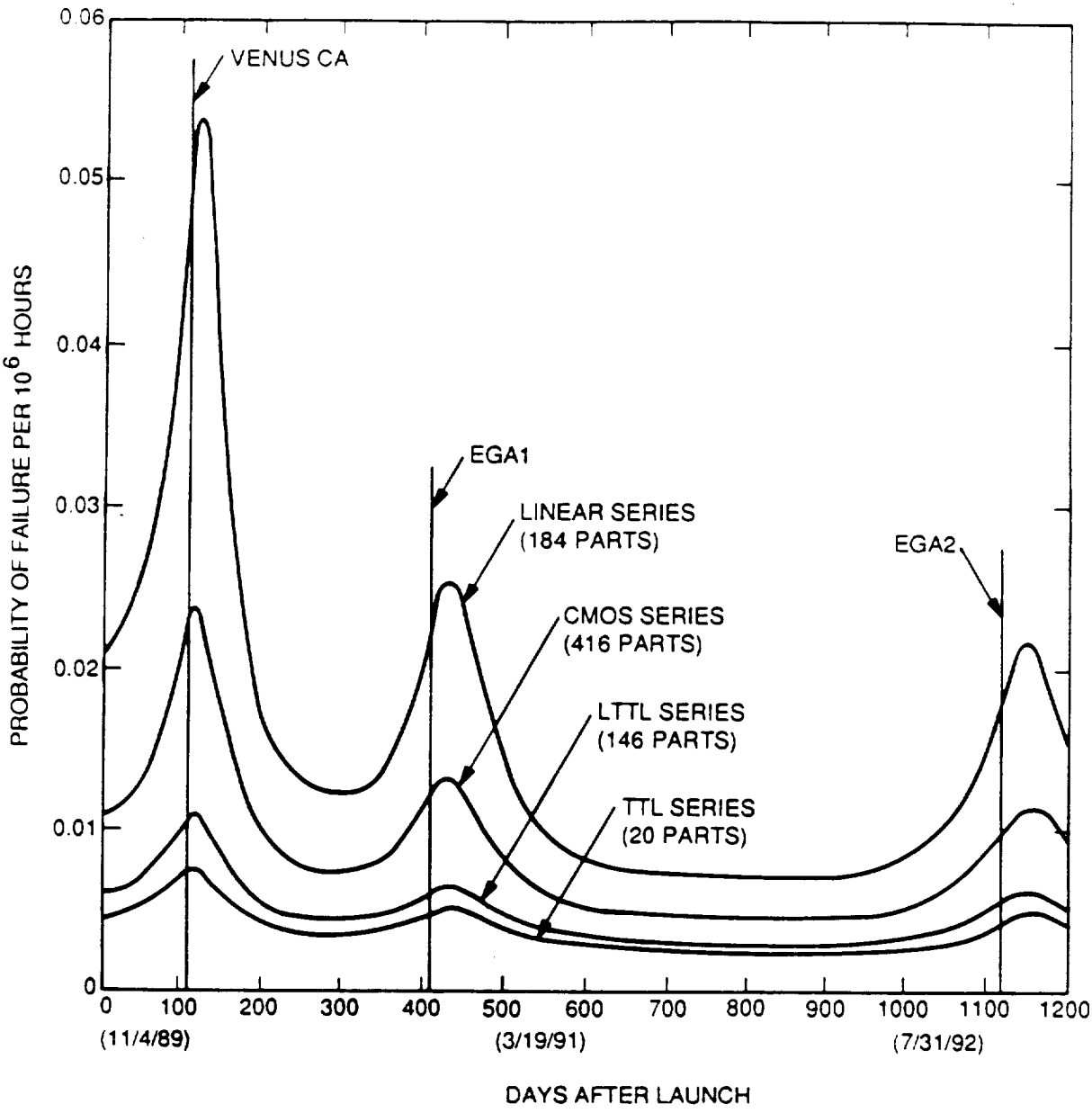


Figure A-10. Probability of Failure for AACS Logic Devices for 90° Off-Sun Attitude Based on Methods of MIL-STD-217E

Table A-15. Probability of Failure Due to Off-Sun Thermal Failure -- Tank Rupture Resulting in the Following ΔV During the Following Mission Phases

RELATIVE TO S/C WHICH IS 90° TO SUN			1.6 TO 14 m/s
	VENUS CA TO EGA1		
	AXIAL+ Z	$0° < \theta < 30°$	
	MIXED	$30° < \theta < 60°$	
	LATERAL	$60° < \theta < 120°$	6.4×10^{-9}
	MIXED	$120° < \theta < 150°$	
	AXIAL - Z	$150° < \theta < 180°$	
	PROBABILITY OF NO RECOVERY = 1		
	EGA1 TO EGA1 + 100 DAYS		
	AXIAL+ Z	$0° < \theta < 30°$	
	MIXED	$30° < \theta < 60°$	
	LATERAL	$60° < \theta < 120°$	4.1×10^{-9}
	MIXED	$120° < \theta < 150°$	
	AXIAL - Z	$150° < \theta < 180°$	
	PROBABILITY OF NO RECOVERY = 1		
	EGA1 + 100 DAYS TO EGA2 - 10 DAYS		
	AXIAL+ Z	$0° < \theta < 30°$	
	MIXED	$30° < \theta < 60°$	
	LATERAL	$60° < \theta < 120°$	7.3×10^{-10}
	MIXED	$120° < \theta < 150°$	
	AXIAL - Z	$150° < \theta < 180°$	
	PROBABILITY OF NO RECOVERY = 1		

Table A-15. Probability of Failure Due to Off-Sun Thermal Failure Tank Rupture Resulting in the Following ΔV During the Following Mission Phases (Continued)

			1.6 TO 14 m/s
	EGA2 - 10 DAYS TO EGA2		
RELATIVE TO S/C WHICH IS 90° TO SUN	AXIAL+Z	$0° < \theta < 30°$	
	MIXED	$30° < \theta < 60°$	
	LATERAL	$60° < \theta < 120°$	5.6×10^{-9}
	MIXED	$120° < \theta < 150°$	
	AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = 1

Table A-16. Probability of Failure Due to Off-Sun Thermal Failure -- Parts Resulting in the Following ΔV During the Following Mission Phases

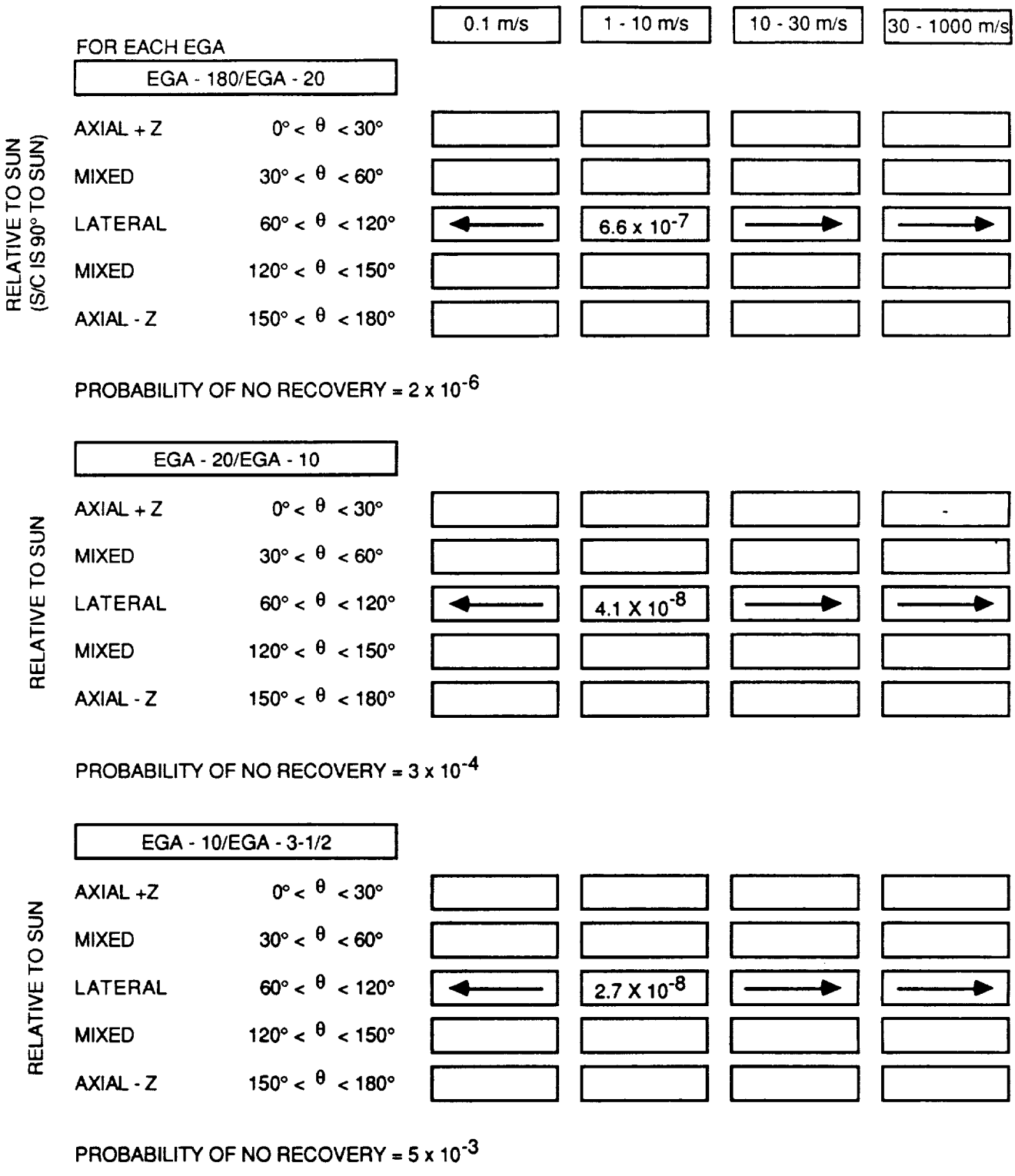


Table A-16. Probability of Failure Due to Off-Sun Thermal Failure -- Parts Resulting in the Following ΔV During the Following Mission Phases (Continued)

A.2 ENVIRONMENTAL FAILURES

A.2.1 Meteoroid Damage to Propellant Tanks.

Although no interplanetary spacecraft is known to have suffered catastrophic meteoroid damage, meteoroid-induced failure of a Galileo propellant tank poses a potential Earth impact risk. The failure has the potential of expelling several hundred kilograms of propellant, imparting velocity to the spacecraft and enveloping it in a cloud of caustic vapor. The resulting spacecraft damage makes a recovery maneuver unlikely.

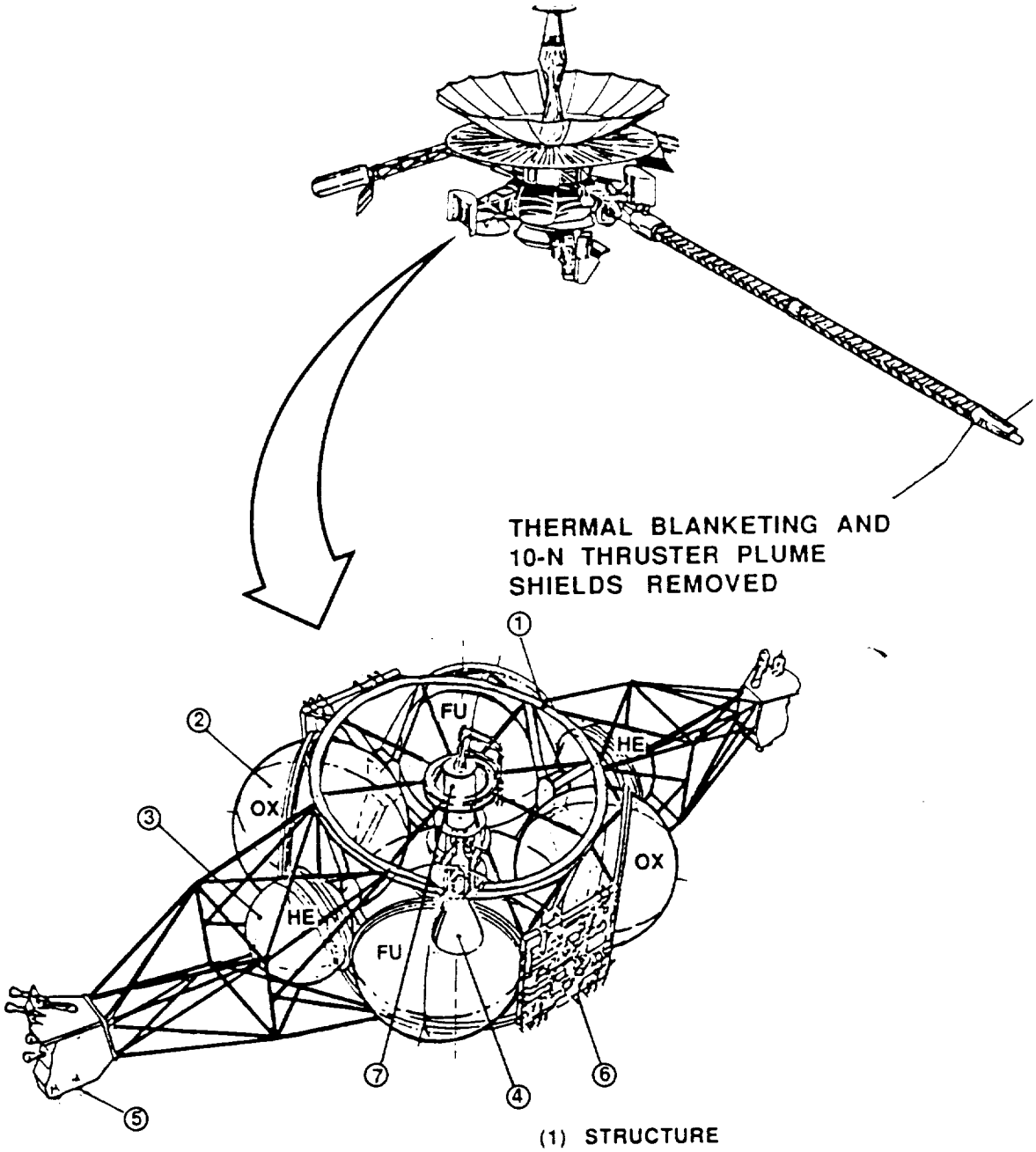
As later sections will show, empirical knowledge of the solar system's meteoroid distribution is incomplete, especially for meteoroids large enough to harm propellant tanks. Extensive data exist for large meteors (based on lunar and Martian cratering) and for fine meteoric dust (estimated from zodiacal light observations), but little is available for intermediate sizes. Since the meteoroid sizes relevant to spacecraft failures fall in this intermediate range, this report must rely on available models which employ interpolations to predict the likelihood of tank failure. Where assumptions must be made, they have been chosen to err conservatively, overestimating rather than underestimating the risk.

To assist in the estimation of the critical mass to puncture a Galileo propellant tank, JPL contracted with H. Swift, an expert in the field of hypervelocity impacts, to provide a detailed description of the mechanics of meteoroid penetration. This study, reviewed by other experts in the field, provides the best understanding to date of the interaction of micrometeoroids with fluid-filled tank walls and bumper shields.

The question of how a micrometeoroid penetration affects a tank was also the subject of significant analyses. These included studies of fluid flow from a punctured tank, effects of multiple tank failures including combustion and propellant discharge, effects of propellant escape on spacecraft dynamics, and vulnerability of blankets and electronics to free propellants. The findings of all of these studies contributed to the results in the following sections.

The Galileo propulsion system uses four spherical titanium tanks to carry Galileo's 955 kg propellant supply. The fuel (monomethyl hydrazine) and oxidizer (nitrogen tetroxide) reside in tank pairs as shown in Figure A-11. The innermost propellant tank halves are completely enclosed by solid spacecraft structure; thruster booms and electronic bays partially surround the outermost tank halves, but otherwise only their multi-layer insulation (MLI) lies between them and space (see Table A-17).

In flight, the spacecraft rotation holds the propellant against the outer tank walls where tubing leads it to the thrusters. Helium pressurant, used to drive the propellant out to the thrusters, fills the ullage volumes, the tanks' remaining capacity, along the inside wall. Together, these fluid/gas vessels operate at pressures between approximately 17 and 20 atmospheres, depending on temperature. Even up through the second Earth encounter, the tanks will still contain nearly their full launch load of propellant, approximately 90% by volume.



(1) STRUCTURE
(2) PROPELLANT TANKS (4)
(3) PRESSURANT TANKS (2)
(4) 400-N ENGINE ASSEMBLY (1)
(5) 10-N THRUSTERS (12), 2 CLUSTERS
(6) PRESSURIZATION & FEED SYSTEM (2)
(7) SPIN BEARING ASSEMBLY (SBA) - ATTITUDE CONTROL HARDWARE

Figure A-11. Propulsion System (RPM) Elements

Table A-17. Characteristics of Galileo RPM Meteoroid Protection

Material	Density gm/cm^3	Thickness cm	No. Layers	Total Areal Density gm/cm^2
		BUMPER SHIELD CHARACTERISTICS		
MYLAR	1.38	6.35×10^{-4}	20	0.01753
KAPTON	1.38	2.54×10^{-3}	4	0.01402
TEFLON	2.00	5.08×10^{-3}	1	0.01016
NYLON NET	0.95	---	21	0.01469
			TOTAL AREAL DENSITY =	0.05640
		TANK CHARACTERISTICS		
		PROPELLANT TANKS (4)		
TITANIUM ALLOY	4.54	0.08	1	0.36320
		PRESSURANT TANKS (2)		
TITANIUM ALLOY	4.54	0.35	1	1.58900
		DIMENSIONS		
	SENSITIVE AREA:		$8.65\ m^2$	
	PROPELLANT TANK DIAMETERS:		0.75 m	
	PRESSURANT TANK DIAMETERS:		0.38 m	
	BLANKET STAND-OFF FROM TANKS:		> 0.1 m	

Figure A-12 shows a simplified picture of how the Galileo propellant tanks interconnect with the rest of the propulsion system. When thruster firings burn off propellant, high pressure helium (about 200 atmospheres at launch) flows through a pressure regulator which expands the helium, lowering the downstream pressure to about 17 atmospheres. Helium pressurant then flows into the propellant tanks through either of two spring-loaded check valves; these valves permit helium to flow into the tank but automatically seal themselves so neither helium nor propellant vapor can flow back out. Once inside the propellant tanks, this new pressurant settles in the ullage volumes, replacing propellant volume lost by firing the thrusters. Fault protection software continuously monitors tank pressures so it can detect and isolate a failed regulator; relief valves, added for the VEEGA mission, protect against overpressures caused by anomalous solar heating of the tanks (see Section A.1.8).

Cometary and asteroidal particles in orbit around the Sun may impact Galileo surfaces and cause damage. Particulate sizes range from dust particles with masses below 10^{-6} g up to km-sized asteroids, while the velocities range from a few km/s up to 50 km/s. Here, the discussion concentrates on particles with masses between 10 and 1000 mg and speeds between about 5 km/s and 30 km/s as these correspond to the approximate range of values associated with the lowest mass particles capable of penetrating Galileo's meteoroid protection and causing an RPM tank failure. Since tank failure due to meteoroid impact represents the only major source of ΔV from meteoroids, particles capable of penetrating the RPM shield are the primary particulate threat to a successful Earth flyby.

A micrometeoroid of sufficient size and velocity will penetrate the micrometeoroid shield, either intact or producing an expanding shell of fluid or debris which penetrates the tank wall. This penetration results either in a hole in the tank of some size or a crack which may propagate to the gas-filled ullage region of the tank, causing a violent tank rupture. Such a tank rupture is likely to involve all four propellant tanks and may result in combustion of propellants in the inner regions of the RPM.

Both tank holes and rupture induced combustion result in an anomalous ΔV imparted to the spacecraft due to the momentum carried off by escaping propellants. The two cases result in similar amounts of ΔV imparted, albeit from very different processes. Therefore, it was not necessary to address the difficult question of which of the processes was most likely. Instead the two were considered equally likely in the analysis, noting that if either process were determined to dominate, the change in the overall Earth impact probability would be negligible.

The failure analysis is described in the following three sections. First, the characterization of the meteoroid environment and the analysis of tank susceptibility to failure will be described and the probability of a tank failure determined. Next, the analysis of the consequences of tank holes and ruptures and the ΔV resulting from these occurrences will be described. In the final section, the calculations leading to probability of failure and resultant ΔV will be summarized.

A.2.1.1 Micrometeoroid Failure Mechanism. This subsection provides an estimate of the threat in terms of the probability that the RPM will be struck by a meteoroid large enough to cause failure during the portion of the Galileo mission between launch and second Earth flyby. Failure probability calculations require meteoroid fluence models as a function of mass and speed (velocity relative to the spacecraft), critical mass (meteoroid size capable of penetrating a tank) as a function of speed, and the exposed sensitive area. Each model will be discussed.

In this analysis, the probabilities for the Galileo trajectory profile in terms of the instantaneous probability of meteoroid penetration will be computed for four different populations. The first is based on the cometary meteoroid model (density of 0.5 g/cm^3) adopted by the Galileo Project following a review by a panel of experts in the field. The second is based on the original NASA guidelines for computing the cometary meteoroid fluence and velocity. The third model, again based on the original NASA guidelines, is used to compute the asteroidal meteoroid component (density of 3.5 g/cm^3). The final model is that for the debris environment around the

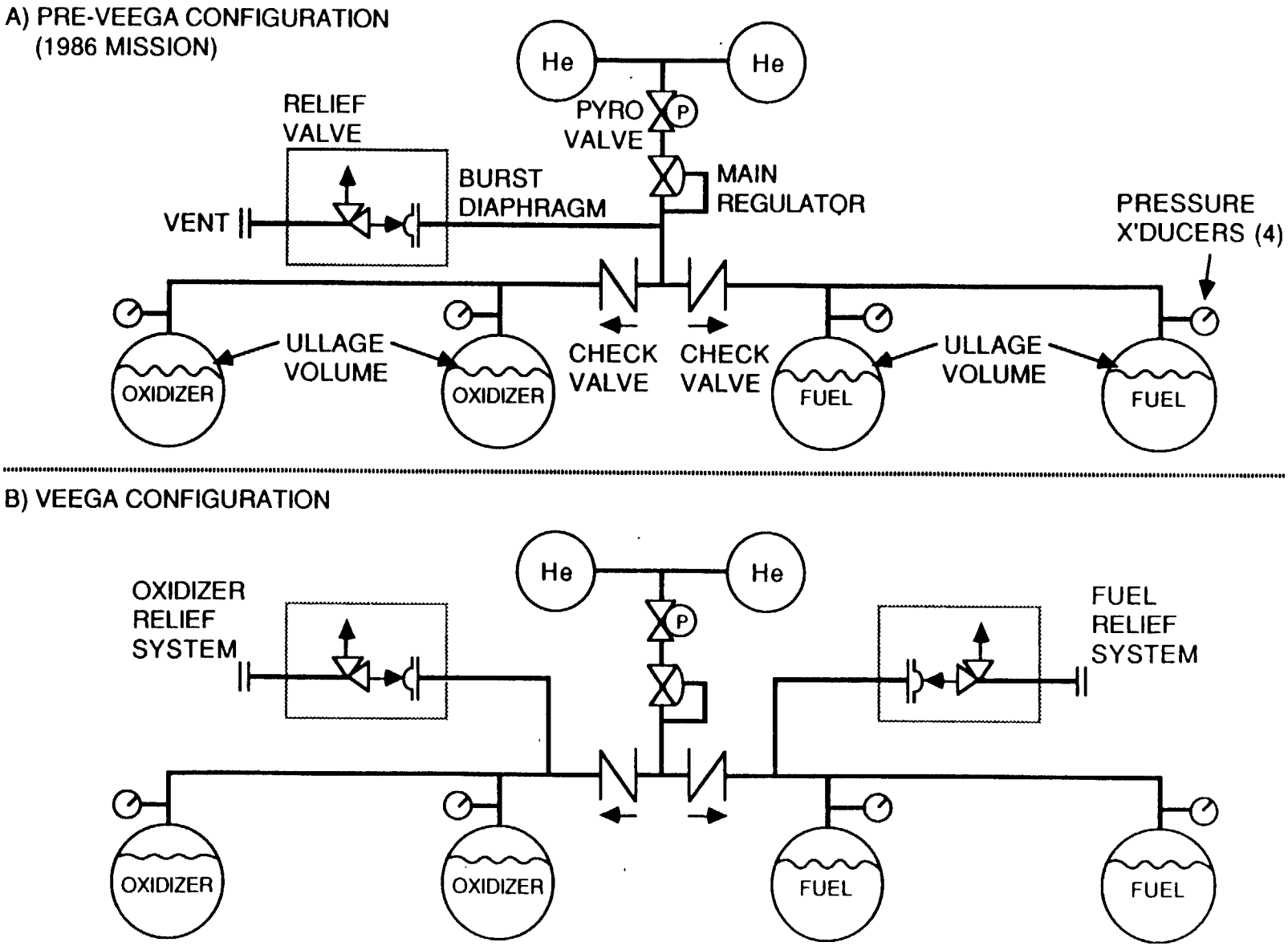


Figure A-12. RPM Pressurization System (Simplified)

Earth. Debris particles are taken to have a density of about 2.8 g/cm^3 -- between that of the cometary and asteroidal debris. The debris model is based on the 1-10 cm NSSR and NORAD observations for the altitude and latitude distribution, and on modelled and measured mass distributions between 500 and 600 km as described in Aguero, R., "Earth Debris Model," JPL IOM 5137-88-118, June 14, 1988. These models are referred to respectively as the Galileo model, NASA cometary model, the NASA asteroidal model, and the debris model.

The interplanetary meteoroid models used here are all based on the NASA cometary and asteroidal models as defined in publications NASA SP-8013, SP-8038, and SP-8042 which date from 1969-1970. (These models are comprehensively described in the referenced NASA documents and will not be discussed further.) Subsequent modification of the two NASA models was carried out by a committee (the Galileo Meteoroid Panel) convened by the Galileo Project Office in 1978-1980 to incorporate the latest Pioneer 10/11 meteoroid data. As the Galileo model has never been formally documented, the major recommendations of the Panel are repeated here:

1) The NASA meteoroid model consists of two populations: cometary (density of 0.5 g/cm^3) and asteroidal (density of 3.5 g/cm^3). Based on the Pioneer 10/11 results which indicated the absence of an asteroidal component at low masses, the panel recommended that only the cometary component be considered.

2) Except for the spatial density, the NASA cometary model was used as the basis for the Galileo Model. The NASA cometary model includes an R-1.5 power dependence of the spatial density on distance. As a conservative assumption, the panel recommended assuming a constant density between 1 and 5 AU for the Galileo model.

3) The constant particle spatial density of the Galileo model was taken to be twice that of the NASA cometary model at 1 AU. (Note: as the original mission did not go inside 1 AU, nothing was decided by the panel for variations within 1 AU. It has, however, been tacitly assumed in the current study that the factor of 2 and constant spatial density should also be applied within 1 AU.)

4) The flux was assumed to be isotropic.

Subsequent work with the Galileo Model has led to this additional assumption:

5) The so-called "Δ factor" in the NASA cometary model which accounts for the distribution of actual spacecraft to meteoroid relative velocities has been eliminated from the Galileo model.

For the purposes of this analysis, the most conservative approach was taken to evaluate the bounding case. The Galileo cometary model as described above was used in conjunction with the NASA asteroidal model. In order to demonstrate the conservatism of these assumptions, the probability of tank failure will be presented for the NASA cometary model as well. As will be shown, the total set of assumptions is more conservative than either the Galileo model or the NASA model taken separately.

The susceptibility of a tank to failure by a micrometeoroid was the subject of extensive study. Analyses used in the past to determine shield thickness such as those by Cour-Palais (AIAA Paper 69-372, 1969 and Int. J. Impact Engng., Vol. 5, pp. 221-237, 1987) were reviewed. However, none of the existing work adequately dealt with a hypervelocity impact to a tank partially filled with liquid and the remainder with pressurized gas. As a result, a study was commissioned to calculate the characteristics of the threshold particle which could penetrate a Galileo Propellant tank. The study was performed by H. Swift, an expert in the field of hypervelocity impacts, and reviewed by Professor T. Ahrens (CIT), another expert in the field, as well as several members of the JPL Technical Staff.

The tanks are protected by a micrometeoroid shield which will be described below. The analysis of the threshold mass and velocity for penetration is determined as a function of the shield parameters and is also described in the following section. The results of the analysis are summarized in the final section.

The MLI enclosing the propellant tanks, as with all Galileo thermal blanketing, provides both thermal control and meteoroid protection. It is made from Kapton plastic sheets and alternate sheets of Mylar and nylon mesh sandwiching a single 2-mil Teflon layer, then stitched together with Dacron thread. To enhance meteoroid protection, fiberglass arches hold the MLI at least 10 cm from the tank walls, giving the blanketed RPM core the appearance of a large inner tube.

Most meteoroids, those weighing in the tens of milligrams or less, vaporize or pulverize on impact with the MLI. Larger, less plentiful meteoroids, around 100 milligrams, may or may not vaporize or pulverize depending upon their velocity and density. In the most extreme and least probable case, the spacecraft will encounter a meteoroid greater than 100 milligrams which perforates the MLI intact.

Vaporized or pulverized meteoroids form a debris cloud upon exiting the MLI. The large gap between the MLI and the tanks allows this debris cloud to disperse over an area of at least several square centimeters before striking a tank wall. Meteoroids of sufficiently low mass and velocity form debris clouds which only briefly deform a tank wall. Larger meteoroids break open tank walls with either a more powerful debris cloud or an intact particle. These specific failures are discussed in more detail in the following material.

Whether a meteoroid will penetrate a tank is a function of its mass and velocity and the characteristics of the tank and shield, including their thicknesses and separation. A kinematic analysis was done on the impacting projectile to determine mass and velocity thresholds for the tank parameters. Cometary and asteroidal meteoroids were treated separately since their different densities, 0.5 and 3.5 gm/cm^3 respectively, affect the thresholds.

The first test of whether an incident particle will cause tank failure is whether it is either fully pulverized or vaporized in passing through the bumper shield. It was found that all cometary meteoroids in the relevant mass range are easily vaporized by the available energy of the collision. Stony, dense asteroidal meteoroids, however, can be treated with confidence as fully crushed only if the shock wave duration is longer than the time it takes the shock wave to pass through the meteoroid. In this case the meteoroid is isostatically or "fully shocked" and disintegrates. Any meteoroid which is not fully shocked is considered to be capable of penetrating a tank.

Fully shocked meteoroids pass from the bumper shield to the tank as an expanding shell of debris. For this debris cloud to penetrate the tank it must satisfy two conditions as it strikes the tank. First, the thickness of the incipient spall, ts, (which is proportional to the wavelength of the shock wave in the tank wall) must be less than the tank wall thickness, tt. This is required to form a reflected tensile shock wave in a region of the wall which is not undergoing the incident compressive shock. Thus, a condition which is denoted by "ts = tt" bounds the region for which a tensile stress exists which will pull material away from the inner surface of the tank. This material is referred to as spall.

The second condition is that the pressure induced by the reflected tensile wave must exceed the tank wall strength. This is referred to as the "no spall" condition. Meteoroids for which the debris cloud meets these two conditions will induce separation of material from the inner tank wall surface.

If this spall removes enough material to exceed the stress tolerance of the tank at its operating pressure, the tank will fail. Otherwise, the spall is termed "acceptable spall."

The results of this analysis are shown in Figure A-13. Separate curves are plotted for cometary (ρ = 0.5 gm/cm^3) and asteroidal (ρ = 3.5 gm/cm^3) meteoroids. The results are also presented for two values of bumper shield and tank separation, S. The minimum value of S is 10 cm, but most of the tank is over 15 cm from the shield. Greater separations result in increased meteoroid thresholds for fully shocked particles since the cloud has more time to diffuse and disperse its momentum. Since at least 90% of the tanks' outward facing surface is greater than 15 cm from the shield, the separation was very conservatively treated as 10% at 10 cm and 90% at 15 cm in determining the threshold meteoroid mass and velocity at a given point in the spacecraft trajectory.

For each of the four combinations of density and spacing, Figure A-13 shows the threshold penetrating meteoroid parameters. The limiting factor in each region of the curves is labelled as described in the previous section. Only asteroidal meteoroids show a "fully shocked" threshold. The "$t_s = t_t$" and "no spall" conditions for spall production are also shown. The "transmitted wave no spall" refers to the "no spall" condition applied to a shock wave that has passed through the fluid inside the tank and reflected off its inside surface. "Acceptable spall" conditions are also shown.

For the pressurant tanks, which contain only gas, more traditional constraints apply. The threshold mass is inversely proportional to velocity in all regions and depends upon the square of the separation.

As just discussed, the critical mass for the existing Galileo configuration was found to vary in a complex fashion with impact velocity, density, and spacing. The probability of an impact of a meteoroid of this mass or larger on the RPM during the VEEGA mission is computed by multiplying the meteoroid fluence by an estimate of the sensitive area of the RPM. To a high degree of accuracy, this cumulative probability of impact of a meteoroid on the Galileo RPM is given by:

$$\text{Prob}(t) = F(t) * A$$

where:

t = elapsed time since launch

F = meteoroid fluence at or above critical mass as a function of time

$$= 0.25 \int_0^t p(t) \langle V(t) \rangle \, dt$$

A = Appropriate sensitive area for Galileo (Table A.17)

p = Spatial density for critical mass at average velocity at time t

$\langle V \rangle$ = Average impact velocity (speed) at time t

The meteoroid fluence as a function of time is derived for each of the four environment models. Specifically, a "p" and a "$\langle V \rangle$" are computed for time steps along the Galileo trajectory and the above equation integrated to give "F" for the appropriate spacing and particle species. The results of this probability of failure calculation will now be presented.

Given the questionable existence of the asteroidal component and the ability to bias the trajectory to limit these effects, cometary meteoroids are the most critical population for the Earth avoidance study. The impact probabilities as a function of mission elapsed time (MET) for the Galileo and NASA Cometary models are plotted in Figure A-14 and listed in Table A-18. These values are derived using the critical mass necessary to penetrate the propellant tanks assuming the MLI is spaced 15 cm away from 90% of the sensitive areas and 10 cm away from the remaining 10%.

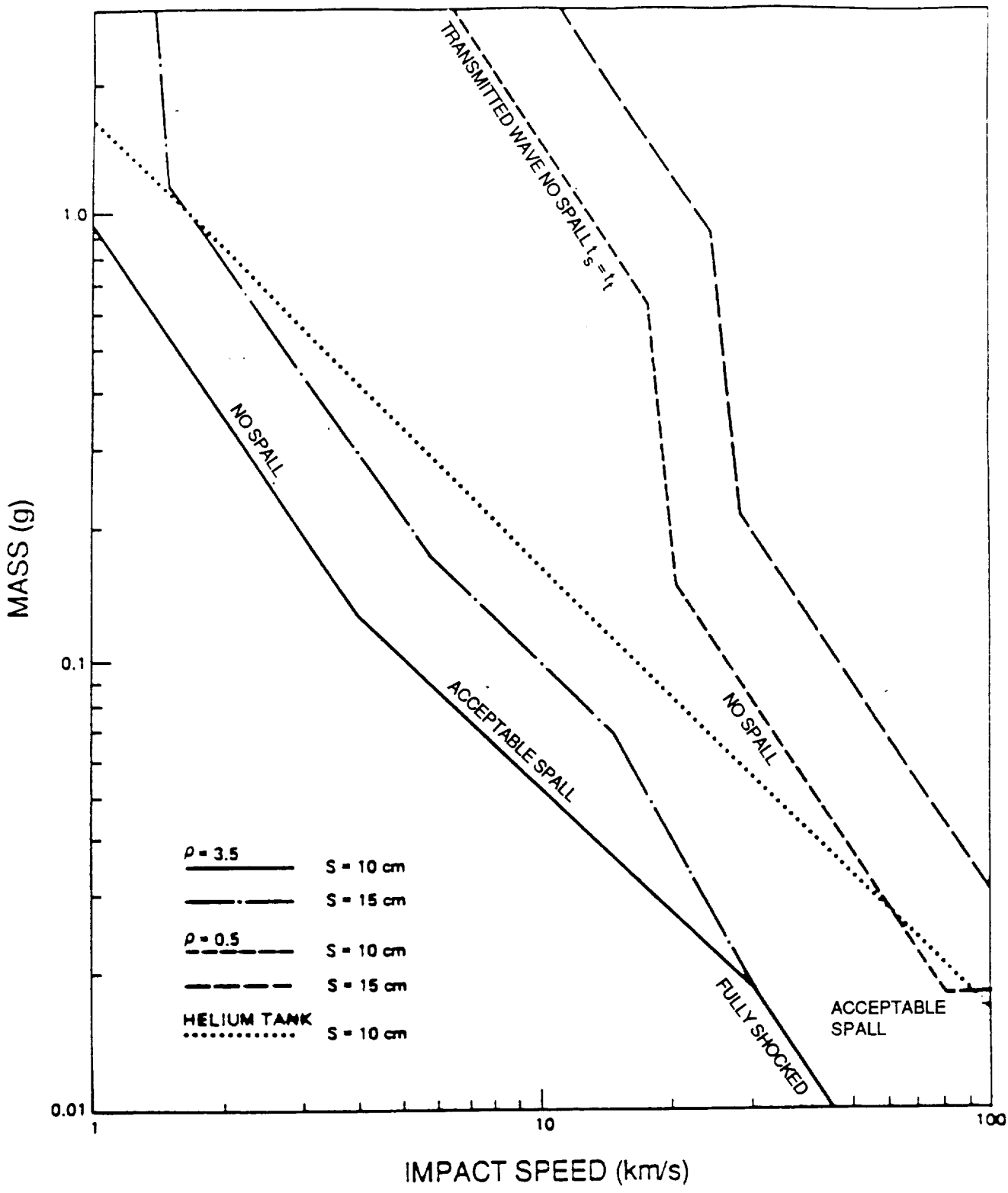


Figure A-13. Variations in Meteoroid Critical Mass for RPM Propellant Tanks

As in the case of the cometary meteoroids, the probability of an asteroidal meteoroid impact is given by the product of the fluence and sensitive area. Unlike the cometary meteoroids, however, the asteroidal component will, if it exists, only be observed in and near the asteroid belts. This behavior is reflected in Figure A-15 where it is clear that, through the time of the second Earth flyby, only between the two flybys is there any risk of encountering this component. The flux is strongly modulated by orbital position, approaching zero near the Earth. In order to guarantee that the total estimated probability of tank failure is an upper bound of the actual probability, this study will assume the existence of the asteroidal component despite the Galileo Meteoroid Panel recommendations. The final probability is listed in Table A-18.

The Earth debris environment resembles the asteroidal component in its behavior. First, the density is quite high (2.8 g/cm^3) so that the critical mass is roughly the same. Secondly, the debris are concentrated only near the Earth so that the flux is non-negligible for only a short time during the two Earth flybys. Similarly, the probability of a propellant tank hit is given by the product of the fluence and sensitive area. This probability is plotted in Figure A-16 where it becomes clear that only for a few minutes during the first and second Earth flybys is there any chance of encountering this component. At this time, the ΔV required to achieve an impacting trajectory is so large that the risk is essentially non-existent. Table A-18 lists the final results for debris impact.

The four propellant tanks are filled with liquids and, as shown in Swift (1988), this critically alters the mass/velocity curves. As a result, the penetration curves are very dependent on the density and other properties of the incoming particles (see Figure A-13). The two pressurant tanks, on the other hand, are filled with gas and therefore respond more like a typical double meteor shield and are nearly independent of the density of the incoming particle. The critical mass/velocity penetration is given by the formula:

$$m_c = 0.0168\ S^2/V$$

where:

m_c = Critical penetration mass (grams)

S = Shield spacing (centimeters)

V = Relative impact velocity (kilometers/second)

The geometry of the helium tank shield is also somewhat simpler than for the propellant tanks, making possible a direct integration of the penetrating fluence per unit area as a function of spacing over the shield surface area. This integration gives the probabilities of failure listed in Table A-18.

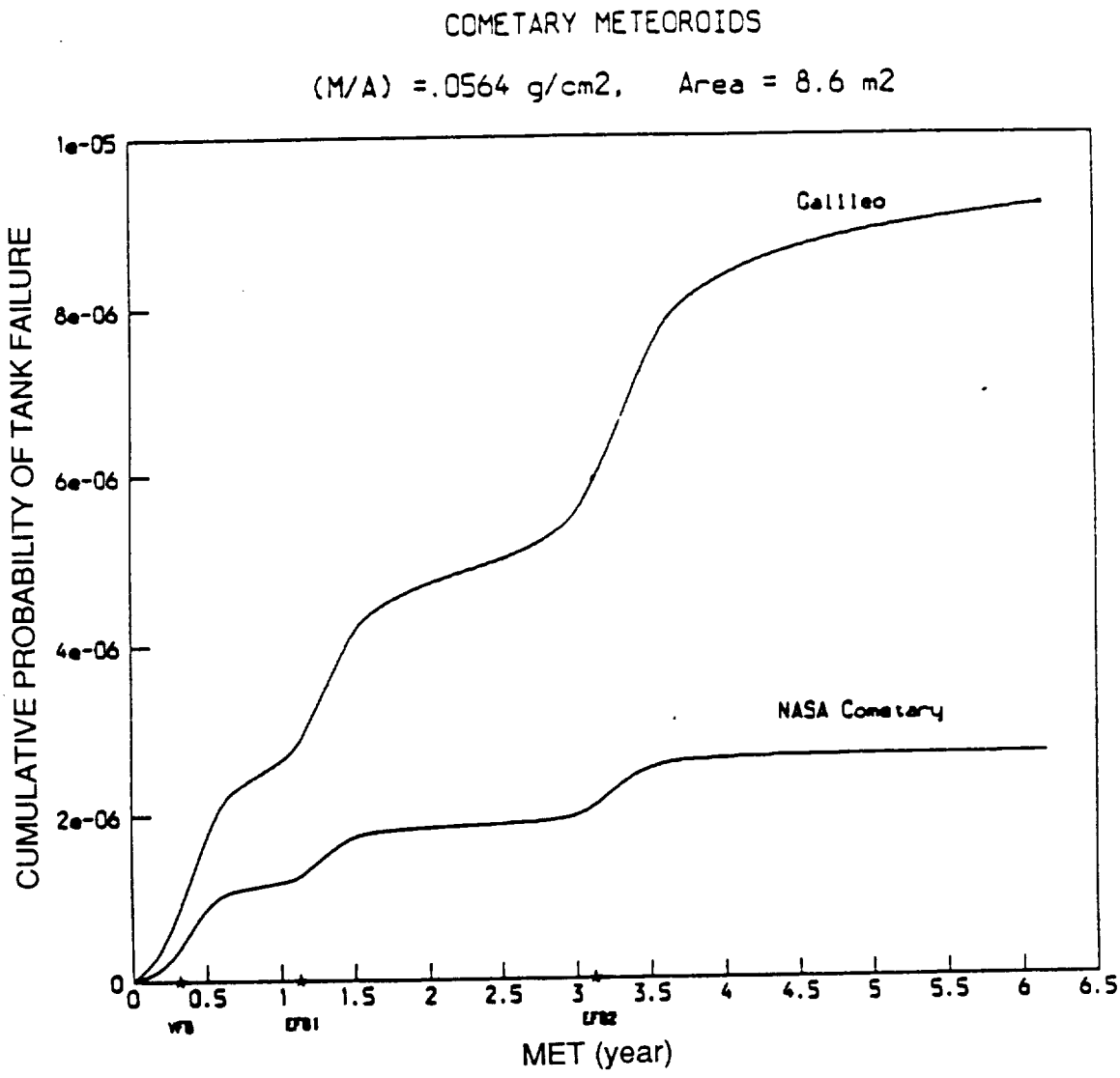


Figure A-14. Variations in Cometary Meteoroid Impact Tank Failure Probability as Function of Mission Elapsed Time (MET)

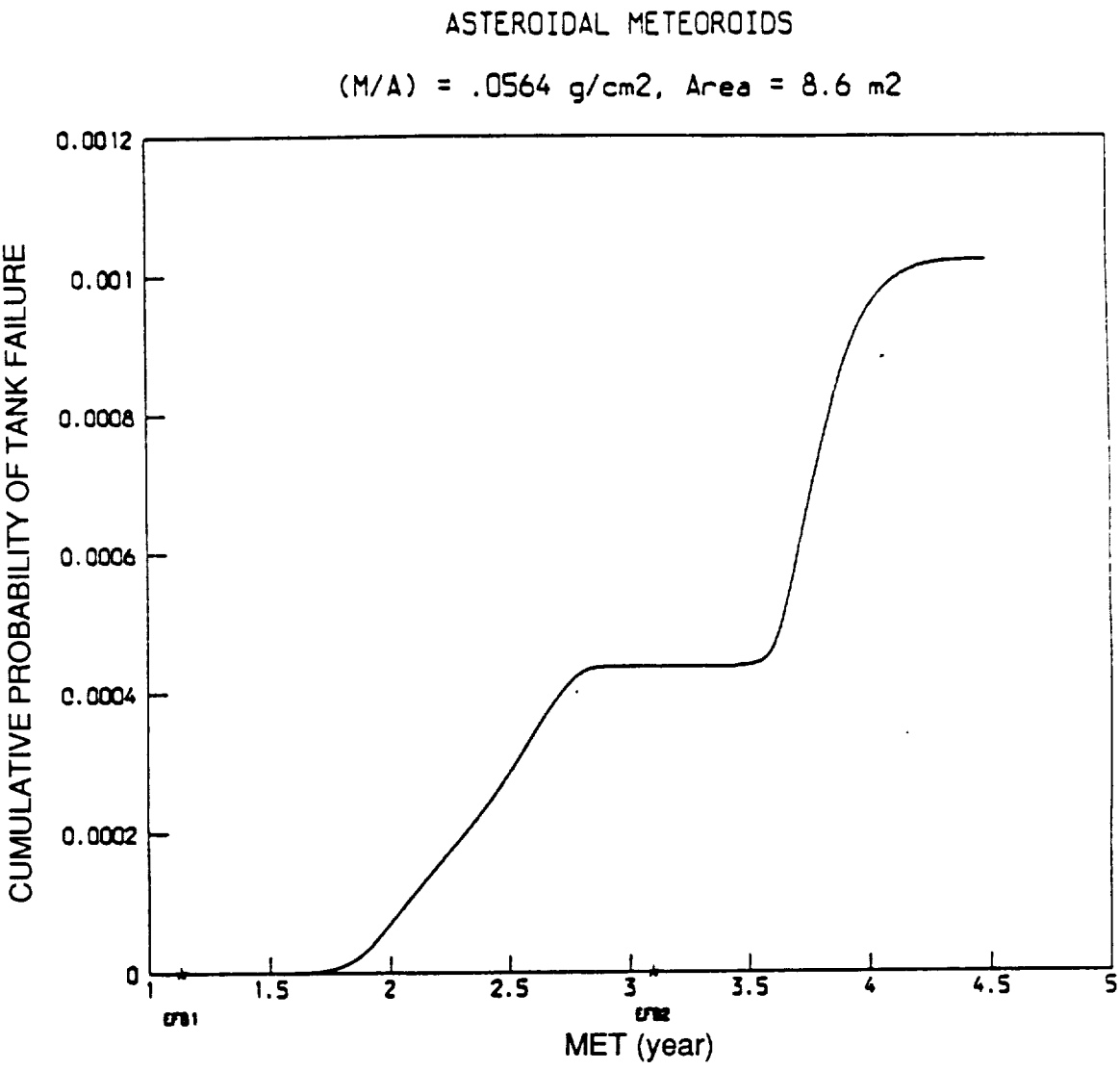


Figure A-15. Variation in Asteroidal Meteoroid Impact Tank Failure Probability as a Function of Mission Elapsed Time (MET)

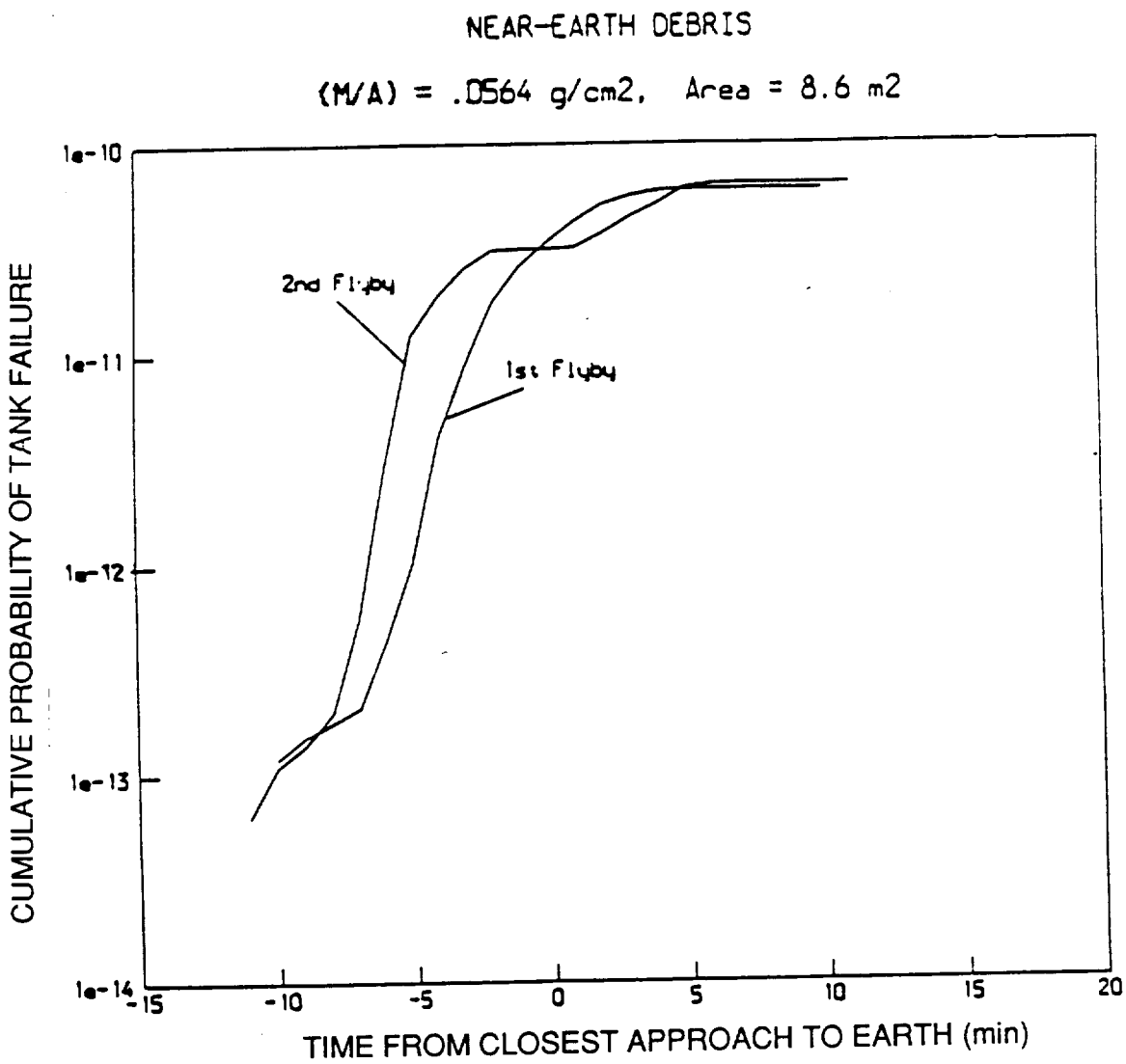


Figure A-16. Variation in Earth Debris Impact Tank Failure Probability as a Function of Time From Closest Approach to Earth

Table A-18. Meteoroid Impact Tank Failure Probabilities for Launch Through Second Earth Flyby: 9 Oct. 1989 - 12 Dec. 1992

System	Probability* of Tank Failure
PROPELLANT TANKS	
Galileo Cometary Model	6.07×10^{-6}
NASA Asteroidal Model	4.37×10^{-4}
Debris Model	1.40×10^{-10}
PRESSURANT TANKS	
Galileo Cometary Model	3.06×10^{-6}
NASA Asteroidal Model	1.23×10^{-5}

---

*Assumes 7.74 m^2 of area at 15 cm spacing, 0.86 m^2 of area at 10 cm spacing and 0.0564 gm/cm^2 of shielding.

Table A-18 and Figures A-14 through A-16 show the probabilities of RPM penetration by a micrometeoroid. Since the probability of an Earth debris hit is so low, it will be ignored. The remaining results are combined to produce a total probability of RPM penetration by a cometary meteoroid, 9.13×10^{-6}, and by an asteroidal meteoroid, 4.49×10^{-4}. For the former case, although the actual failure probability varies slightly from launch to EGA2, this probability was modeled as uniform over this period. For the latter case, the failure risk is only present while in the asteroid belt between 1.5 and 4.2 AU and is fairly constant during that period. The failure is, therefore, treated as equally likely from launch plus 1.8 years to launch plus 2.7 years and zero at all other times before the second Earth encounter. These data are summarized in Table A-19.

A.2.1.2 Consequences of Tank Failure. Empirical observations show that tank punctures behave differently for liquid-filled and gas-filled volumes. Walls of liquid-filled pressure vessels tend to crack, while the walls of gas-filled vessels are more likely to shatter. Discussions with industry experts led to the conclusion that meteoroid penetration of a Galileo propellant tank, containing mostly liquid with a small gas-filled ullage, would cause the tank to fail as if liquid-filled, but the tank may also exhibit gas-filled behavior when the resulting crack contacts the ullage bubble. The following scenario (Figure A-17) describes the best estimate of how a nearly full propellant tank behaves when struck by debris from meteoroids above the critical mass.

Since blanketing disperses the debris striking the tank walls, a large meteoroid impact forms a crack rather than a pinhole. Internal pressures rapidly enlarge the crack into a "clamshell" rupture. Once started, this crack, spreading at near-sonic velocity, randomly propagates around the tank. If the crack enters the ullage bubble region, compressed helium gas escapes into the RPM central cavity, immediately relieving internal pressures. The sudden gas release may shatter that part of the tank wall. Crack propagation and possible gas release occur before most of the tank's propellant can exit the tank.

Table A-19. Probability of RPM Tank Failure Due to Impact by a Micrometeoroid Between Launch and Second Earth Flyby

Meteoroid Source	Total Failure Probability	Period of Vulnerability	Probability per day
Cometary	9.13×10^{-6}	Launch to EGA2	7.8×10^{-9}
Asteroidal	4.49×10^{-4}	Launch + 1.8 yrs to launch + 2.7 yrs	1.4×10^{-6}

As a minimum, a failed propellant tank will be left with a large gash opened toward space. If the crack extends to the ullage bubble, the tank may also have a large hole where the gas release fragmented the interior wall. Either way, the tank releases its contents.

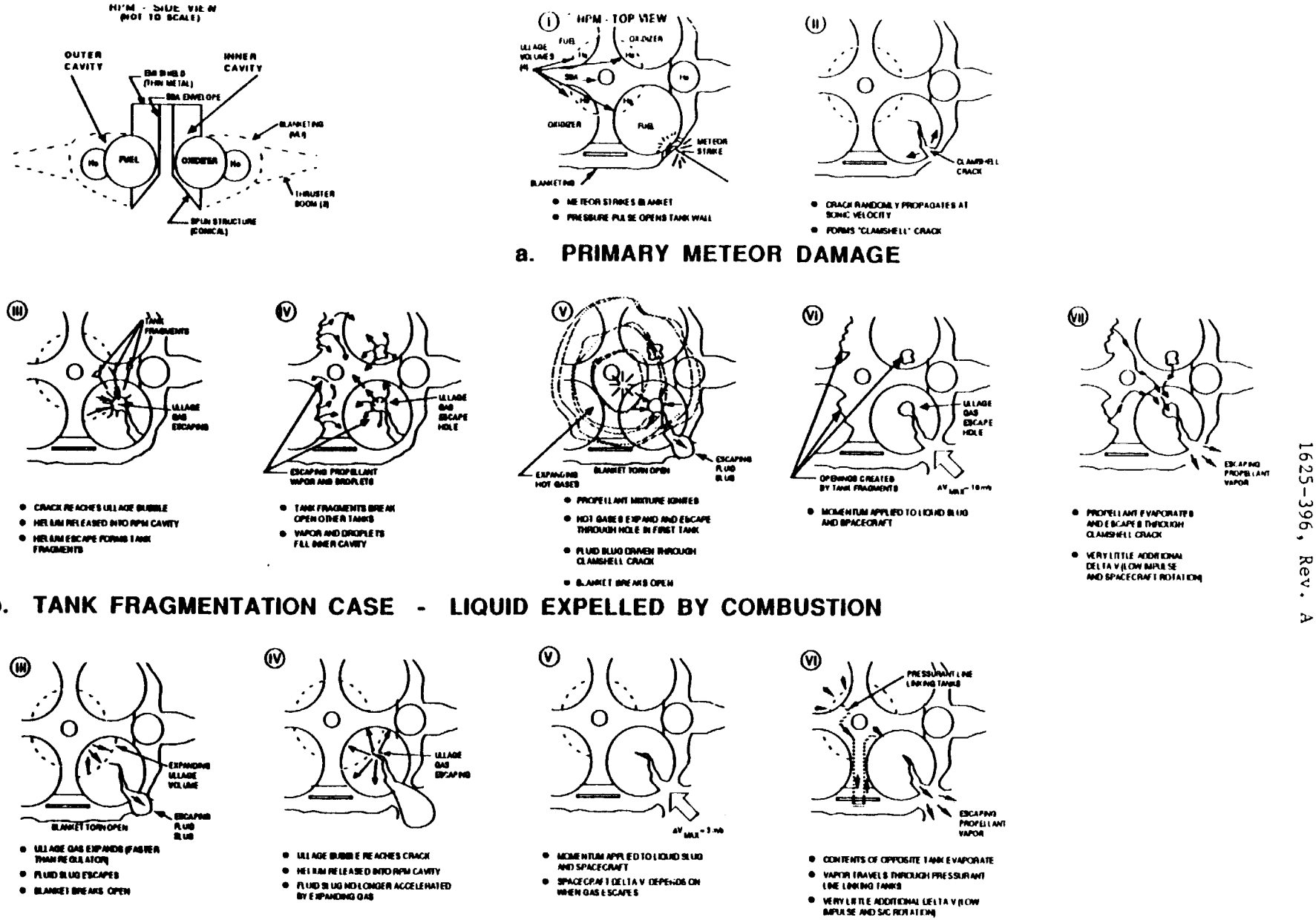


Figure A-17. Tank Rupture and Propellant Expulsion

In the case of a single tank failure, the liquid is pushed out of the tank by the pressurant behind it. This propellant discharge is the mechanism by which ΔV is applied to the spacecraft.

If a propellant tank crack contacts the ullage region before internal pressures have been relieved, rapid gas release may shatter part of the tank wall. As compressed helium escapes into the central cavity, it carries off any titanium fragments and accelerates them to high speeds. This tank wall "shrapnel" readily broaches any tanks it encounters (see Figure A-17b).

The conditions for creating shrapnel from a mixed fluid/gas-filled tank are complex and not well understood. Some researchers believe that no shrapnel will be created while others regard shrapnel generation as nearly certain. No relevant empirical data could be found to resolve this question. Therefore, to adopt the more conservative approach, this report assumes meteoroid damage to a propellant tank will be as likely to produce shrapnel as not. Subsequent sections show that these two failure scenarios lead to ΔV distributions of roughly similar magnitude.

Unlike propellant tanks, pressurant tanks fail in a well-defined manner. Based on empirical data, meteoroid damage to these tanks results in violent releases of high pressure helium (about 200 atmospheres versus less than 20 atmospheres for the propellant tanks) and shattering of the vessel. High-speed titanium pieces scatter in all directions. Given their proximity to the RPM central body, pressurant tank shards are almost certain to penetrate adjacent fuel and oxidizer tanks. Nearby blanketing will also be ripped open, exposing damaged tanks to space.

When one or more propellant tanks break open, the energy released drives liquid propellant through the exterior clamshell crack and so perturbs the spacecraft's velocity. This energy comes from either fuel and oxidizer combustion in the the case of multiple tank failures or discharge of pressurized fuel, oxidizer, or helium in the case of single tank failures.

The presence or absence of propellant tank shrapnel determines which energy source dominates. For example, combustion requires propellant mixing in a confined volume like the RPM central cavity. This only occurs if a damaged propellant tank releases shrapnel. Since this scenario releases the damaged tank's compressed helium before the liquid slug can accelerate outward, only combustion effects impart thrust. If, on the other hand, the meteoroid-stricken tank releases no shrapnel, damage is confined to that single tank; propellant pushed out by the discharge of compressed helium pressurant is the only significant source of thrust.

Combustion requires fuel and oxidizer to mix together; neither component by itself releases chemical energy by exposure to a vacuum or contact with spacecraft surfaces. Propellant mixing by direct meteoroid penetration of two tanks is virtually impossible since the meteoroid would have to penetrate the MLI, the tank wall, and still traverse a large volume of energy-absorbing liquid before exiting the opposite tank wall with sufficient energy to break another tank.

A far more plausible scenario presumes that the meteoroid-stricken tank releases wall fragments upon contact of the clamshell crack with the ullage volume; this shrapnel then strikes and gouges tanks containing dissimilar propellant (that is, fuel tank fragments damage an oxidizer tank or vice-versa). With both liquid fuel and oxidizer contacting hard vacuum, the exposed surfaces of the propellants "flash vaporize" and rapidly fill the RPM central cavity with propellant vapors.

Upon reaching an ignition pressure of approximately 0.2 psi, the vapor mixture burns, creating hot gases which drive the tank's fluid slug through the outboard clamshell crack. The MLI offers little resistance and the sudden impulse propels the spacecraft laterally. With the fluid slug expelled, the large cracks in the tank vent the central cavity; internal pressures immediately return to hard vacuum, extinguishing further combustion.

Upon expelling the fluid slug, the cavity releases its propellant vapor. Meanwhile, the regulator works at its maximum flow rate to release the contents of both pressurant tanks over a period of about half an hour. This helium expulsion has little thrust and most of that is smeared out by spacecraft rotation. Likewise, the evaporation and release of the remaining propellant imparts negligible net thrust.

For this scenario, combustion energy depends on the vapor mass reacting inside the central cavity. The amount of propellant vapors filling the cavity is limited by the volume of the cavity (32.5 ft^3) and by the thermodynamic properties of the propellants at ambient temperature. The vapor pressures of the fuel and oxidizer are 1 psia and 15 psia, respectively, at ambient temperature. Since oxidizer has a higher vapor pressure than fuel, the cavity will be rich in oxidizer vapor with the availability of fuel vapor limiting the combustion energy released. Even assuming perfect mixing prior to ignition, the amount of fuel and oxidizer reacting together comprise a small percentage of the RPM's total propellant. At the propellant vapor pressures, the vapor mixture in the cavity will contain 0.18 lbm of fuel and 6.5 lbm of oxidizer.

In the vapor combustion case, the RPM central cavity is treated as a rigid, gas-tight chamber whose only escape path is created by expelling a propellant slug. Using these assumptions, a peak combustion pressure of 103 psia is predicted for the RPM central cavity. In fact, the central cavity contains many vent paths through surrounding structure which will partially relieve internal pressure as the slug is expelled. Furthermore, a large barrier enclosing the top cavity is made from thin metal which will probably be blown out by the combustion. These effects reduce the energy imparted to the propellant slug and thus lower the resulting ΔV imparted to the spacecraft. For conservatism and to simplify calculations, these effects were deliberately excluded from the combustion model.

Another more speculative scenario presumes the broken propellant tanks release most of their contents as liquid droplets into the central cavity. Ordinarily, spacecraft rotation would tend to keep liquid away from the central cavity, but some liquid release can not be ruled out. Droplets expelled into the cavity will either partially or completely vaporize and help pressurize the volume. Due to heat lost from the liquid by flash vaporization, smaller droplets freeze into solid crystals.

When dissimilar liquid droplets collide at sufficient speed, the transient pressure pulse causes their contacting surfaces to burn. Unlike rocket engines, which tightly confine propellants during burning, droplets colliding in the RPM central cavity will blow apart by the energy released at initial contact. Experimental data confirm that combining liquid propellants in this manner releases only a small percentage of the total chemical energy available (less than 0.3% of the chemical energy of the propellants).

The combustion energy released by droplet collision depends on the liquid mass thrown into the central cavity and the probability that a given pair of dissimilar droplets will collide at speeds sufficient for combustion. Given the haphazard way tanks release their contents, accurate estimates of the amount of energy generated are virtually impossible to derive. To bound the problem, analysts estimated the propulsive effects by assuming the maximum energy release possible from bulk impingement and mixing of the spacecraft's propellants in the central cavity and having the resulting combustion occur instantaneously and without venting -- clearly very conservative assumptions. Using these assumptions, a peak combustion pressure of 580 psia is predicted for the RPM central cavity.

The case of pressurant tanks damaging adjacent propellant tanks is special in that both fuel and oxidizer tanks are broken open on their outer hemispheres. The same scenarios apply as before except that two tanks will be initially ruptured instead of one. Outside, fuel and oxidizer vapors will be rapidly released from the ruptured tanks. Since the pressurant tank rupture will have blown away most of the nearby blanketing, exterior propellant vapors vent directly to space. Without containment, these vapors cannot build up to ignition pressure. Therefore, external combustion will not take place.

For the reasons given above, the report treats pressurant tank impacts as equivalent in consequence to propellant tank impacts.

Even in the absence of combustion, tank ruptures can impart velocity by expelling a tank's pressurized liquid contents, much like "water rockets" sold as children's toys (see Figure A-17). If a meteoroid opens a tank, and the crack does not propagate to the ullage volume, then the compressed gas discharges and drives the liquid slug out at high speed. The MLI offers little resistance. Expulsion is so rapid (about one second to empty the tank), the regulator cannot keep up with the pressure loss created by the expanding ullage bubble. In the end, the energy stored by the ullage volume's helium gas (about 17 atmospheres pressure) is released as kinetic energy to both the spacecraft and fluid slug. The spacecraft acquires a velocity change, primarily in the lateral direction (see Figure A-17c).

Upon releasing most of its liquid contents, the tank immediately loses its propellant vapor. The regulator now works at its maximum flow rate to release the contents of both pressurant tanks over a period of about half an hour. The helium expulsion has little thrust and most of that is smeared out by spacecraft rotation. If, on the other hand, the tank's crack does extend to the ullage volume, the consequences will be very different. Crack propagation is so rapid that most propellant will still be in the tank when the pressurized gas is released into the RPM central cavity. In this case, the tank's energy is dissipated by blowing helium pressurant into the RPM central cavity. With the pressurant gone before the propellant can fully escape, the fluid slug accumulates little momentum and the fluid merely oozes out the crack. This has little effect on spacecraft velocity.

Propellant residing in the outermost portion of the tank may remain after liquid expulsion. Liquid propellant exposed to vacuum, whether it is in the damaged or the undamaged tank connected to it, slowly boils away (the undamaged tank, having a thin tube which constricts evacuation, will take at least four days to empty). The release is so slow and the thrust so small that the spacecraft spin-rate smears out any lateral component; furthermore, the thrust efficiency of the evaporating propellant is so low that any axial component created by the orientation of the escape paths will be insignificant. Thus, evaporating propellant adds little or no velocity change to the spacecraft.

In summary, velocity imparted to the spacecraft strongly depends on where the crack propagates. Cracks which stay on the outer tank hemisphere release most of the tank's propellant before the helium can escape. Cracks reaching the gas relieves the internal pressure before most of the propellant can be accelerated outward.

A.2.1.3 Resultant ΔV. As mentioned earlier, propellant tank shrapnel must form for combustion to take place, otherwise velocity will be imparted by pressurant discharge only. Since the incidence of shrapnel cannot be demonstrated with certainty, this analysis uses identical likelihoods of shrapnel and combustion as no shrapnel and fluid expulsion.

In the case where combustion occurs, the energy released within the RPM central cavity is virtually identical for either a fuel tank or oxidizer tank broken open by a micrometeoroid. However, since the oxidizer mass is significantly greater than the fuel mass, expelling the oxidizer slug of a single tank imparts slightly more velocity to the spacecraft than a fuel slug. Calculations show that even if worst-case vapor combustion is present, damaging a fuel tank laterally propels the spacecraft no more than 3 meters/second while damaging an oxidizer tank produces no more than 4 meters/second.

A ΔV resulting from liquid combustion was modelled by assuming the maximum energy release possible from bulk impingement and mixing of the propellants in the RPM central cavity. This yields a lateral spacecraft ΔV of about 8 m/s for a damaged fuel tank and 10 meters/second for a damaged oxidizer tank.

Vapor combustion is judged to be significantly more likely than liquid combustion. Analysts estimate that the conditional probability that combustion produces a spacecraft ΔV of 3.5 meters/second (mean of fuel and oxidizer tank ΔVs) or less is about 90%. The probability that the ΔV will be 9 meters/second or less (massive fluid combustion) is at least 99.9%. Based on these probabilities, a probability distribution can be constructed for the resultant ΔV as shown in Figure A-19. This distribution approximates the effects of other phenomena, such as venting within the central cavity (tending to reduce the net ΔV) and combinations of vapor and fluid combustion. The direction of the spacecraft ΔV is determined to be in the lateral direction.

In the case where there is no combustion, and the ΔV results from propellant discharge, the worst-case ΔV results from assuming that the propagating crack never reaches the ullage bubble, allowing the compressed gas within the tank to transfer all its stored energy into

propelling the fluid slug. Table A-20 summarizes the sources of impulse to the spacecraft. Due to spacecraft rotation, only the first two will produce non-negligible ΔV. In this worst-case, the expelled propellant produces a ΔV of 3.2 meters/second.

In reality, the tank's pressurant will always be released before all propellant is expelled. As discussed previously, the crack may propagate to the ullage bubble and release the pressurant even before the propellant has had a chance to escape and build up momentum. In other cases, where the crack doesn't quite reach the ullage bubble, the ullage bubble will expand as rapidly as propellant is expelled. At some point it will reach the edge of the crack, escape, and stop imparting momentum to the fluid slug. Thus, the spacecraft's ΔV is probabilistic and can be much less than the worst case. Based on the considerations given earlier, the study team used a worst-case velocity magnitude distribution which is uniformly distributed between 0 and 3.2 meters/second.

The exact direction of the ΔV is a function of the meteoroid strike location and crack orientation. There will always be a strong lateral component, but a crack formed predominantly in an upper or lower hemisphere will produce some axial component as well. Clearly, this too is probabilistic. Given that the spacecraft structure above and below the RPM protects the tanks at their poles, the study team used a distribution of angular direction which is uniform between 60^{o} and 120^{o} from the spacecraft's spin axis.

A.2.1.4 Probability of Recovery. Depending on the meteoroid's entry point and the type of propellant expulsion, spacecraft attitude and spin rate will be perturbed. During parts of the VEEGA trajectory where telecommunications performance is weak, an unplanned attitude change could disrupt the data link between the ground and the spacecraft. In this case, the ground must rely on the spacecraft's fault protection software to autonomously switch antennas and restore communications.

If the spacecraft spins up or spins down during propellant expulsion, AACS fault protection will respond by firing a spin thruster to bring rotation back to nominal. However, the rapid loss of pressurant coupled with the propellant loss will probably make this ineffectual. If the spacecraft spins up to 14 rpm, parts of spacecraft structure, especially the magnetometer boom, will break off and leave a large residual wobble (see

Table A-20. Spacecraft Impulse Resulting From Propellant Discharge

Escaping Fluid	Impulse (Newton-seconds)	Impulse Duration (seconds)
First Tank Liquid	7820	1.0
First Tank Vapor	480	0.6
Pressurant	1220	2070
Second Tank Vapor	12000	>100 hours

Section A.1.5 for a description of how the RTGs are retained in spite of structural failures). If the final spin-rate is near zero, the spacecraft will be dynamically unstable and prone to tumbling.

Fuel or oxidizer can chemically attack the Dacron threads used to hold the MLI together. If liquid droplets land on blanketing threads, the MLI layers will weaken and, if the exposed area is large, cause thermal blanketing to fall off. Without thermal protection, exposed electronics bays will cool to inoperable temperatures.

Chemical reactions with the propellants can harm spacecraft cabling and electronics. The oxidizer is particularly caustic and attacks most plastics (Teflon is immune, however). Where non-Teflon insulating materials are exposed to the oxidizer, they will slowly erode. Power and signals necessary to control the spacecraft could short out. By comparison, the fuel is much more benign, softening plastics rather than eroding them.

Besides these effects, recovery depends upon limiting the damage to only the fuel tanks or only the oxidizer tanks. If a propellant tank failure produces high velocity fragments, all propellant tanks may be damaged. Fragmentation of a pressurant tank is almost certain to damage at least one fuel and one oxidizer tank.

Quantifying the remote recovery prospects for these failures is extremely difficult and subject to large uncertainties; therefore, this report models the likelihood of recovery from meteoroid-induced tank failure as zero.

A.2.1.5 Summary. The risk of RPM tank damage due to micrometeoroids has been determined to come from two sources, cometary meteoroids and asteroidal meteoroids. While the threat from the cometary component is present and relatively uniform for the entire first three years of the mission, the asteroidal threat is only present for less than a year while in the asteroid belt. The probabilities per day of the micrometeoroid damage for both components are shown in Figure A-18. As can be seen, the asteroidal risk, when present, is over two orders of magnitude greater than the cometary risk.

If an RPM tank fails due to a micrometeoroid hit, two possible failure scenarios have been determined. In the first, only a single propellant tank is involved, and ΔV is imparted to the spacecraft due to the momentum carried off by escaping propellants. The ΔV imparted to the spacecraft is equally likely to have magnitudes from zero to 3.2 m/s and directions between 60^{o} and 120^{o} to the spacecraft spin axis. The magnitude distribution is shown in Figure A-19. In the other case, tank damage results in a crack propagating to the ullage region followed by a tank rupture, fragments from which rupture the remaining propellant tanks. Ensuing combustion pushes propellants out through the initially struck tank, imparting ΔV to the spacecraft through momentum transfer. The magnitude of the ΔV is modelled as a distribution which peaks at about 2 m/s as shown in Figure A-19. The direction of the ΔV is 90^{o} to the spacecraft spin axis.

The two cases of velocity distribution have been taken to be equally likely. If one should subsequently be shown to prevail, the effect on the Earth avoidance probability will be negligible since they are so similar.

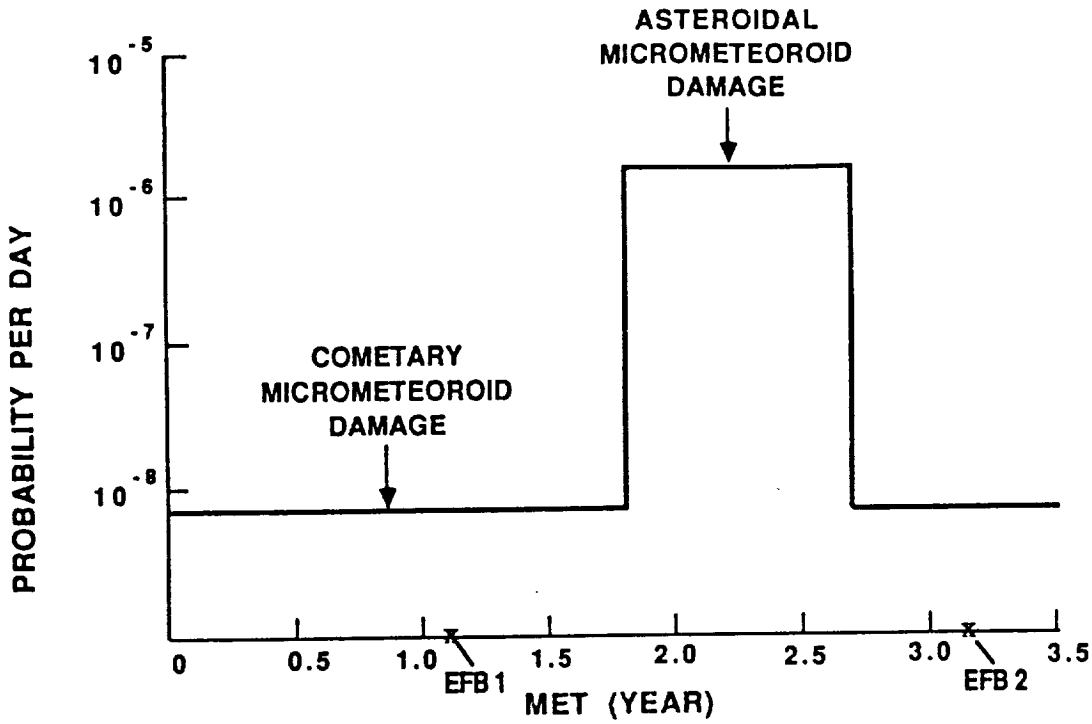


Figure A-18. Probability Per Day of Micrometeoroid Damage to Propellant Tanks

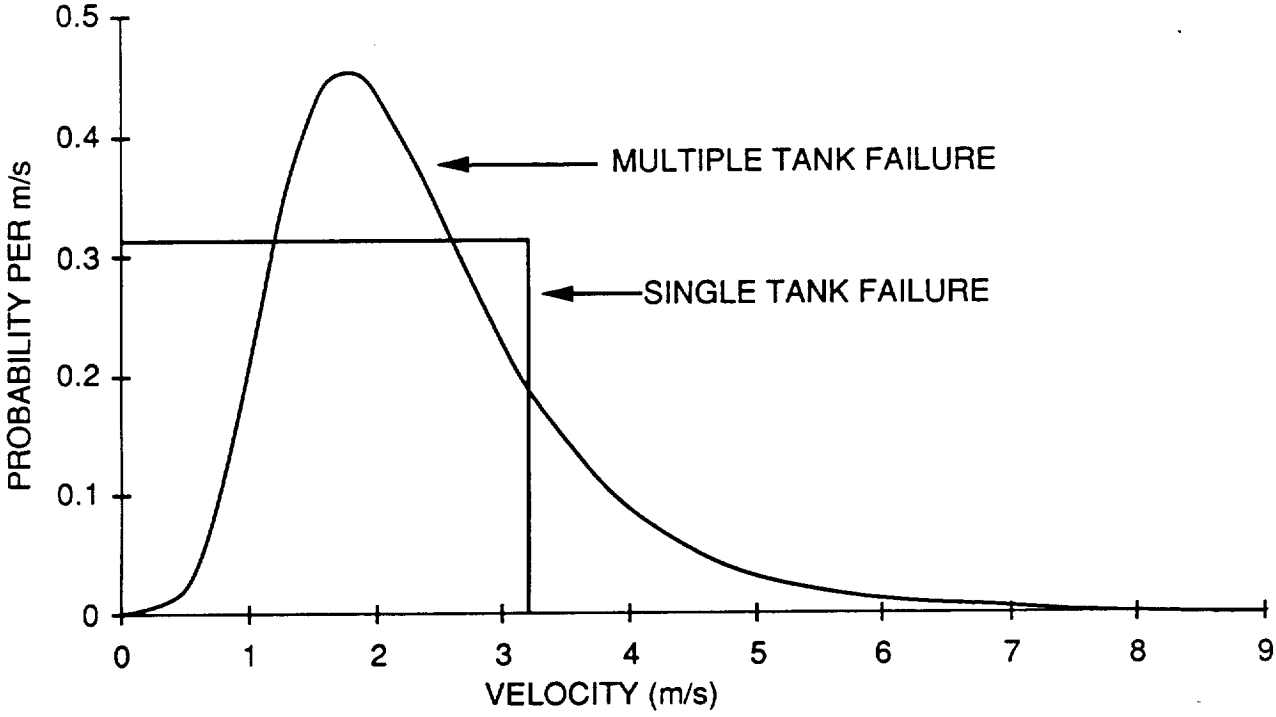


Figure A-19. Velocity Distribution for Failures Resulting From Micrometeoroid Impacts

A.2.2 Radiation

Although radiation has been carefully considered for its effects on mission reliability, it poses a negligible threat to Earth avoidance. This is due to the fact that the majority of the radiative effects that will be seen by the spacecraft occur in the vicinity of Jupiter. Galileo, like Voyager, is radiation hardened to the Jovian environment. The dose that it will receive by the time of the second Earth encounter is less than 5% of the total dose designed for in the entire mission. As will be discussed in this section, Earth avoidance protection from the two principal radiative effects, total dose and single event upsets, requires only a small fraction of the design margin that is available to withstand the Jovian environment. As a result, the probabilities of an anomalous ΔV resulting from these two effects are $<10^{-7}$ and $<2 \times 10^{-5}$ per TCM, respectively. In each case the standard recovery probabilities apply.

As electronic components have grown smaller and have reduced their operating voltages, their susceptibility to radiation damage has increased. The principle forms of this damage fall into five categories: total dose ionization effects, displacement damage, single event upsets (SEUs), signal interference, and latchup. Latchup (where the radiation alters the actual electronic circuit) has been shown not to be a problem for Galileo parts. Displacement damage (where the atoms in the device are physically displaced by impacting particles) caused by protons and neutrons was studied by the Project, and findings indicate that no Galileo systems that could cause a significant ΔV are impacted. Signal interference (perhaps through a light flash in the star scanner due to passage of a cosmic ray) is also not believed to be a likely source of ΔV. This section will therefore concentrate on total dose and single event upsets. In particular, the probability of occurrence of each failure mechanism will be discussed and estimates of potential ΔV provided.

A.2.2.1 Total Dose Ionization Damage. A primary mission concern for Galileo is that long term exposure to the ambient radiation environment will result in various dose-dependent failure mechanisms. Here "dosage" will be assumed to be the energy deposited in a material due to the slowing of charged particles as they pass through the material. Although long term changes in structural material properties could be important due to this effect, most critical to the Galileo mission are effects such as ionization on solid state electronic components due to prolonged exposure to the high energy particles. Typically, the IC part characteristics will change with increasing dose until the part fails to perform properly. Figure A-20 illustrates this for a representative electronic component. As should be clear, even with parts from the same manufacturer as shown in Figure A-20 and same batch, the failure point as a function of total radiation dosage can vary from device to device by as much as a factor of 40%. The time to failure will be greatly dependent on the part type, manufacturer, shielding, radiation spectrum, exposure rate, and even operating cycle. The picture is further complicated because parts will fail over the course of the mission due not only to radiation effects but also thermal effects due to heating.

For reference, there are approximately 75,000 individual ICs on Galileo and roughly 500 part types. Each part has its own unique radiation shielding and dose-failure characteristics. For example, the softest part is predicted to fail at only 16 krad dose while the hardest parts did not fail at doses in excess of 150 krad. The end of mission dose that these parts are expected to survive, behind Galileo's average 2.1 g/cm^2 of shielding, is about 75 krad. Although the probability of failure of these parts due to radiation is typically assumed to follow a normal or log-normal distribution around a fixed design dose, this can vary depending on part history. Here the typical Galileo radiation design margin (RDM) of 2 (150 krad) to 3 (225 krad) will be ignored. It is assumed instead, as a more conservative estimate, that Galileo parts will fail with a log-normal distribution in dosage peaking at a total mission dose (shielded) of 75 krad (RDM of 1) and a log-normal standard deviation of factor 1.4. Figure A-21 plots log-normal probability density and integral probability distributions for a part having these properties.

The estimate presented here is conservative since typical Galileo parts, behind average shielding, have been carefully selected to withstand over 150 krad (RDM of 2). Individual parts softer than this level have been further protected by adding a spot radiation shield to withstand from 150 krad to, in the case of the softest parts, 225 krad (RDM of 3). The predicted total dose from solar flares (95% confidence level), Earth's radiation belts, and solar wind/cosmic rays gives a 3.3 krad dose behind Galileo's 2.1 g/cm^2 of shielding at about 6 years of mission elapsed time (MET), Table A-21. Thus, assuming a worst-case scenario of RDM 1 (or a failure level of 75 krad shielded) and a 1.4 standard deviation factor around this value for an individual part, a dose of 6 krad or more would be required to give a probability of failure (Figure A-21) of 1e-12 for a given part. For 75,000 parts, this would be about 1 x 10^{-7}. For the probability to approach 1, the dose would have to exceed 15 krad behind 2.1 g/cm^2 for a part to fail due to radiation in the transit phase. Thus, part failures due to radiation dosage are highly unlikely (less than 1 x 10^{-7}) until following JOI as the dosage is far too low to affect even marginal parts.

A.2.2.2 Single Event Upsets. Very high energy particles such as cosmic ray heavy ions, heavy ions at Jupiter, and solar flare protons above several MeV per nucleon can deposit sufficient energy in materials to cause light flashes in optics and logic upsets in ICs. These upsets result in signal interference and "soft errors"--errors that are transitory and can be corrected by software. As it is difficult to shield against these effects except for the lowest energy particles, some SEUs must be tolerated during a mission. Of the effects, the random bit flips associated with logic upsets in Random Access Memory (RAM) circuits and similar ICs which could affect control programs are the most serious (light flashes are considered to be interference effects ignored here, see earlier). "Voting" and/or constant monitoring of RAM are common stop-gap measures used to limit the worst effects of this interaction. Despite these fixes, several spacecraft have still exhibited problems with SEUs. A particularly severe example has been the TDRS spacecraft which has about 10 serious SEUs per month. It has been necessary to check TDRS memory several times a day for SEUs and then reinitialize the memory if any are detected to prevent loss of vehicle control. Galileo's memories most likely to result in anomalous thrust due to SEUs are those in the AACS. Propulsion drive electronic (PDE) logic has also been investigated, but was determined to be immune to SEUs. For Galileo, a careful evaluation of the AACS by Burdick et al. (1986) has shown that SEUs could be a concern throughout the mission.

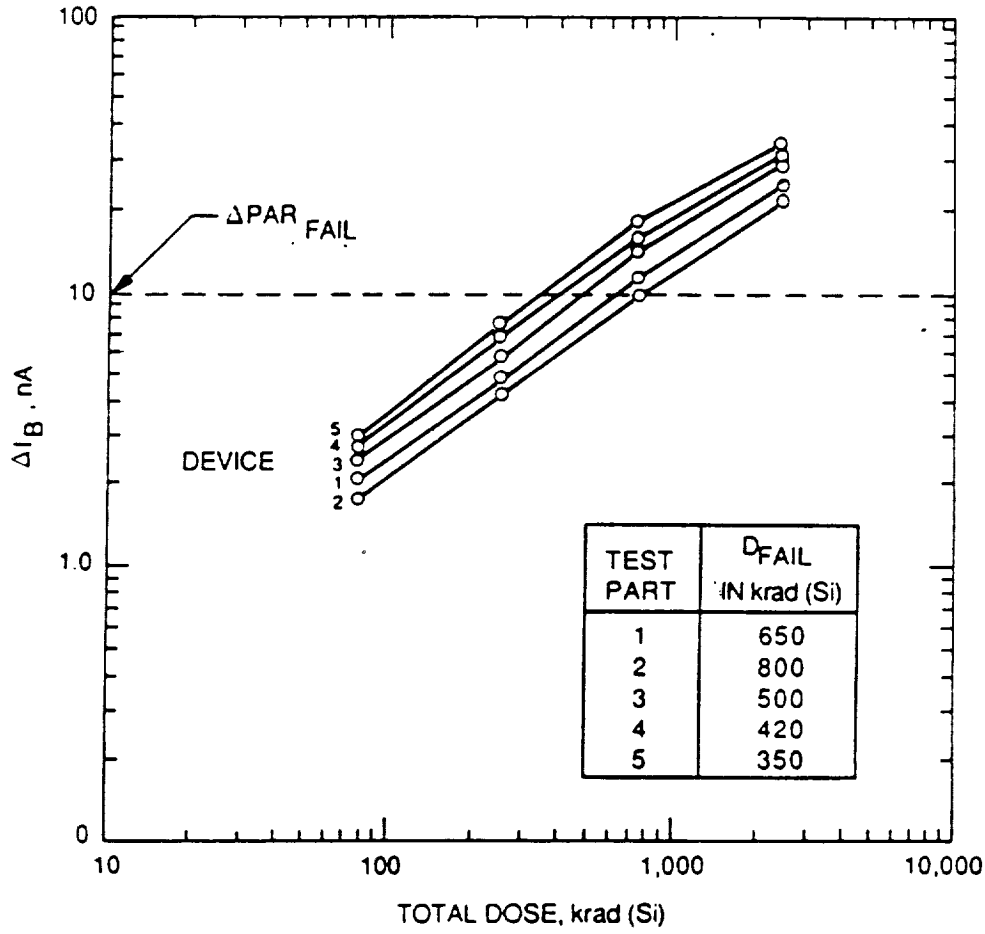


Figure A-20. ΔIB Versus Total Dose for LM108 Amplifiers

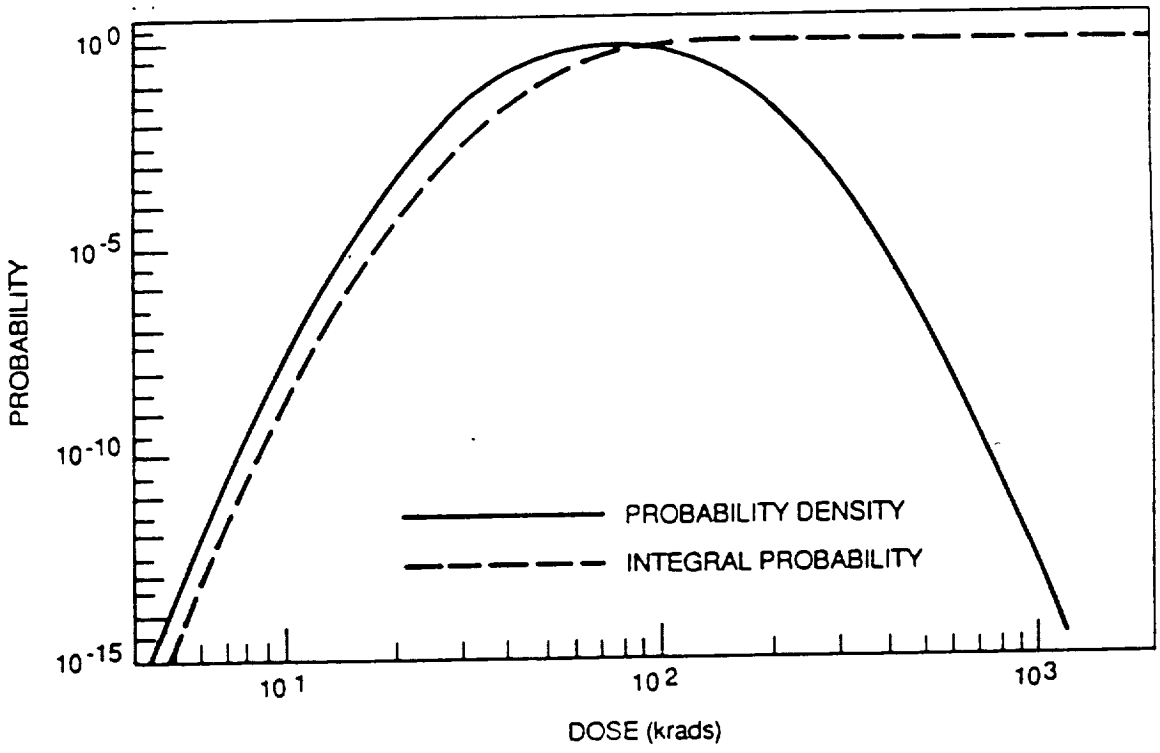


Figure A-21. Integral Probability and Probability Density for 75 krad Part With 1.4 Factor

SEU events are, aside from solar flare effects, equally likely at all portions of the VEEGA mission (there may be slight increase in the vicinity of Earth's radiation belts, but these are ignored here). Solar flare proton fluxes, for the largest events, constitute an additional, unpredictable threat. The probability of an SEU affecting AACS has been conservatively estimated from a low of about 1 error per several years for the cosmic ray background to 1 every few minutes for anomalously large solar flares. Solar flares, for Earth impact studies, will be assumed to occur randomly in time (there is evidence that solar flares are not truly random but occur primarily within +3-4 years of solar cycle maximum) and to last for 1-2 days. For estimation purposes, as a very conservative estimate, 7 ordinary flares (100% probability) as used in the Burdick et al. study and 1 anomalously large solar flare (with 33% probability) could be assumed for the 3.5 year VEEGA mission phase. A plot of the probability of an anomalously large flare occurring during the planned Galileo mission is shown in Figure A-22.

Table A-21. Galileo Total Dose Behind 2.1-g/cm^2 (300-mil) Shielding as a Function of Mission Time

Mission Phase	S_{MIN}	Dosage (Rads-Si) Al/Si Sph. Shell	S_{MAX}
0 to 107 min	0.8		0.8
0 to VFB			
CR + SW		7.3	
Solar Flare (95%)		575	
VFB - EFB1			
CR + SW		16.95	
Solar Flare (95%)		1080	
Earth Flyby 1 (± 70 min)	4.2		4.3
EFB1 - EFB2			
CR + SW		16.95	
Solar Flare (95%)		1060	
Earth Flyby 2 (± 66 min)	2.0		2.1
EFB2 - JOI (N5.3 AU)			
CR + SW		9.52	
Solar Flare (95%)		557	
TOTAL	7.0	3322	7.2

For solar flares the Feynman model was used, which takes into account the so-called "AL" flares as part of the normal population of flares.

Soft errors are, by their definition, recoverable. Thus the induced programming error could be corrected. The probability of a correction of the effect is, as discussed in Burdick et al. (1986) and elsewhere, very much a function of mission phase and the type of error. Typical recovery times range from hours to days depending on a variety of variables. Fortunately, many SEUs will be corrected in the normal operations of the system or will have no effect (see later). Thus, the probability of recovery ranges from near 0 during Jupiter injection to 1 during cruise.

A.2.2.3 Probability Analysis for Failure. As the only failure believed to have a significant chance of causing a ΔV is an SEU in the AACS, the following analysis will only consider this area. Following the procedure laid out in Burdick et al. (1986), SEU rates for the AACS have been estimated for the new VEEGA mission. The following parts were assumed to be sensitive to SEU:

AACS UNIT	IC Name	Number of Devices
MDR	25LS374	1
AOR	54S374	1
RUPT	AM2914	4
MEM1	54LS373	1
MEM3	54LS373	1
MEM5	54LS373	1
MEM8	54LS373	1

The upset tables of Burdick et al. were computed under the conservative assumption that only those units that contained these devices would experience SEUs. The rates used for incident radiation were those used by Burdick et al. (Note: recent rate estimates are a factor of 2-3 lower for flares and about 4 higher for cosmic rays -- which are not important -- making the old rates a more conservative estimate.)

By way of summary, if SEUs in the "miss" and "no effect" categories are ignored, the total AACS upset rates in terms of times between events were, assuming a box shield:

Galactic Cosmic Rays	30 yrs/event
Typical Solar Flare	2 days/event
Anomalously Large Flare	10 minutes/event

These rates are believed to be accurate to within a factor of 3 for the solar flares. They are conservative since they include all SEUs except those in the "miss" and "no effect" categories (see later). Thus, it can be concluded that galactic cosmic rays will, conservatively, contribute only 1 or 2 SEUs during the mission while a typical solar flare (assume 7 during the VEEGA phase) would contribute perhaps 2 to 3 SEUs during the event (events last about 2 days). An anomalously large flare, on the other hand, could generate several 100 SEUs over its duration.

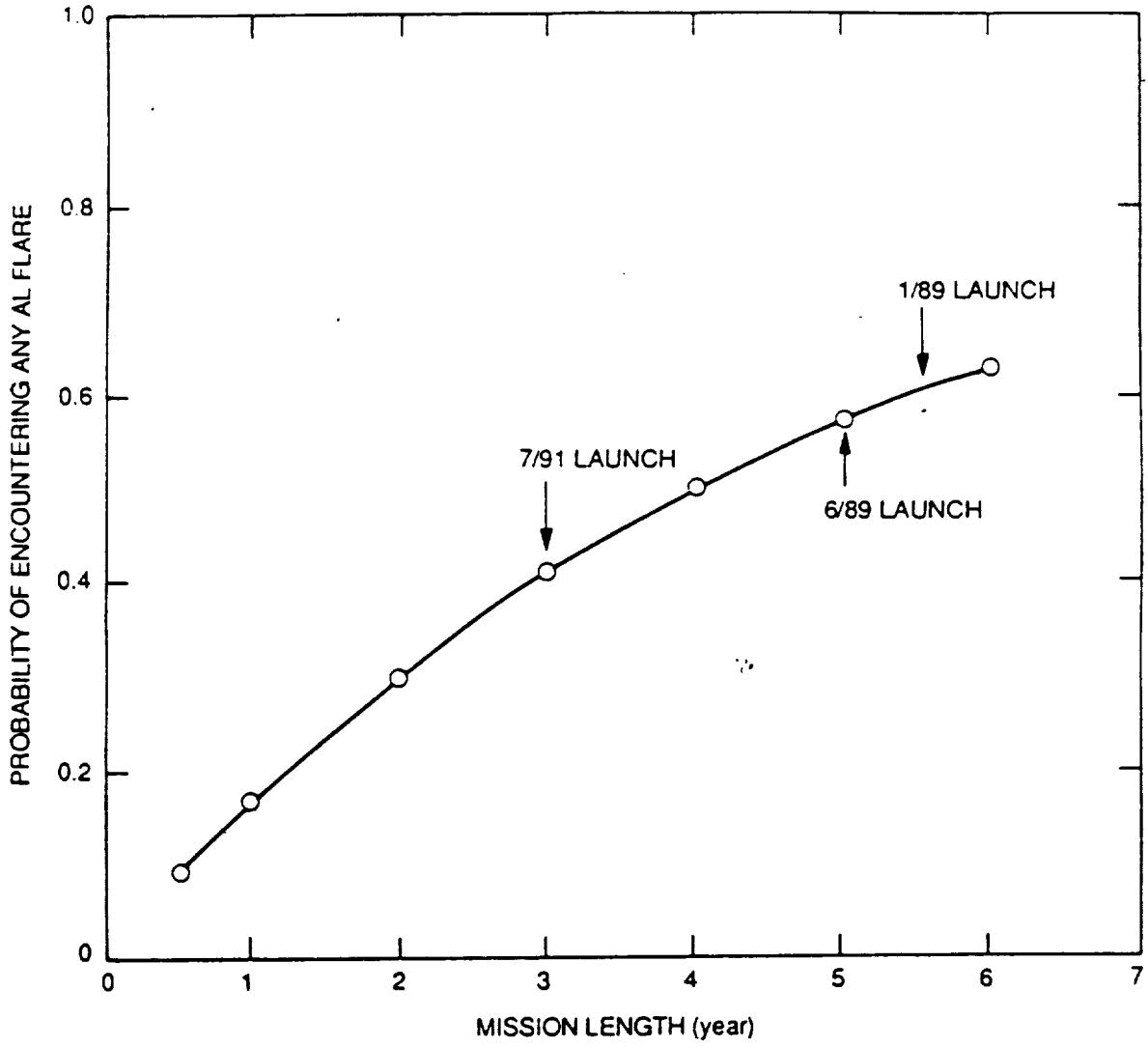


Figure A-22. Probability of AL Flare (3 in Past 21 Years)

Tables A-22, A-23, and A-24 summarize the SEU computations. The format followed is that of the original AACS study with only those units included that are believed to be subject to bit flips. The flip rate per device is multiplied by the percentage time that a flip is expected to have a given effect on the system. These categories of flips are (see Burdick et al. for a detailed explanation of the categories and how the percentages were derived):

Miss	Bit flip results in no possible effect
No Ef	No apparent effect; effect uncertain/not observed
RPT	No apparent effect but flip observed
ACE	Anomalous spacecraft operation
POR	Power on reset

The final flip rates were determined by summing the "RPT", "ACE", and "POR" rates.

A.2.2.4 Summary of Probability. In order to facilitate the computation of the failure probability due to SEUs, the conservative assumption was made that 8 flares (1 anomalously large and 7 "normal" flares) of 2 days duration each would occur--cosmic ray induced SEUs are at such a low rate as to be ignorable for this calculation. This gives a probability of a flare being in progress on any day of 8 flares * 2 days per flare/3.5 years = 0.013. Further, it was assumed that the only way for an anomalous ΔV to result from a flare would be for the flare to occur during a maneuver and for the effect to be a memory change but no POR (a POR would abort the maneuver harmlessly). If a flare were in progress during a maneuver, the most likely way for an anomalous maneuver to occur is for only one or two SEUs to occur. More than this makes it almost certain that a POR will abort the maneuver. From Table A-23, 0.75 of the SEUs that occur and are not "misses" or "no effects" will impact something other than the POR. The probability that a non-POR type SEU affects a burn is the same as for the AACS memory chip failure calculations. That is only failures occurring outside the AACS checksum region will be undetected and uncorrected. Since there are 5,376 bytes outside the total of 32,768 bytes, this gives a probability of 0.16 of a critical byte being hit. A command resulting in an excess burn will be detected and corrected unless it is in the lateral direction. This limits the possibilities for the ΔV magnitude to the lateral burn magnitude range and to a probability of 0.011 as there are only 60 bytes of the 5,376 that could result in such an event. Thus, the probability of an anomalous burn during a trajectory correction maneuver (TCM) due to a solar flare SEU is:

$$\text{Prob} = 0.013 * 0.75 * 0.16 * 0.011 = 1.7 \times 10^{-5}$$

The probability of no recovery is taken to be 2×10^{-6} for TCMs before Earth minus 10 days as it should normally be possible to recover from such an error unless a double fault occurs and 3×10^{-4} for the TCM at Earth minus 10 days since a single fault will prevent recovery (Table A-25).

Table A-22. Galileo AACS SEU Failure Table (Cosmic Rays)

Galactic Cosmic Rays -- Box Shield
(For Units Containing: 54LS373, 25LS374, 54S374, 2914)

SEU Risk Summary for AACS

Category	Miss	No	Rpt	Ace	POR	Ace Effect Obs (Rpt+Ace+POR)
Total Flip Rate: (Flips/sec)	3.7E-7	2.5E-9	4.E-10	1.E-10	4.E-10	9.E-10
Time/Event: (Days)	30.915	4545.5	30458	78850	27557	12225
% Occurrence:	99.076	0.67383	0.10056	0.03885	0.11115	0.25056
P > 1 Disturbance in 100 Days:	0.96063	0.02176	0.00328	0.00127	0.00362	0.00815

Table A-23. Galileo AACS SEU Failure Table (Solar Flare)

Typical Solar Flare -- Box Shield
(For Units Containing: 54LS373, 25LS374, 54S374, 2914)

SEU Risk Summary for AACS

Category	Miss	No	Rpt	Ace	POR	Ace Effect Obs (Rpt+Ace+POR)
Total Flip Rate: (Flips/sec)	0.00012	0.00002	3.7E-6	5.2E-7	1.5E-6	5.7E-6
Time/Event: (Days)	0.10055	0.68094	3.1486	22.316	7.7992	2.0382
% Occurrence:	83.543	12.336	2.6679	0.37642	1.0770	4.1214
P > 1 Disturbance in 100 Days:	1	1	1	0.98868	1.0000	1

Table A-24. Galileo AACS SEU Failure Table (AL Flare)

Anomalous Solar Flare -- Box Shield
(For Units Containing: 54LS373, 25LS374, 54S374, 2914)

SEU Risk Summary for AACS

Category	Miss	No Ace Effect Obs	Rpt	Ace	POR	(Rpt+Ace+POR)
Total Flip Rate: (Flips/sec)	0.03307	0.00486	0.00105	0.00015	0.00042	0.00162
Time/Event: (Days)	0.00035	0.00238	0.01097	0.07885	0.02756	0.00714
% Occurrence:	83.612	12.289	2.6665	0.37112	1.0619	4.0995
P > 1 Disturbance in 100 Days	1	1	1	1	1	1

A.2.3 Spacecraft Charging

Spacecraft charging also does not pose a significant threat to Earth avoidance. Both surface and internal charging have been considered. The most likely threat is from internal charging at the time of the first Earth encounter which may perturb the first TCM thereafter. This occurrence, however, is very unlikely (probability of 1.2×10^{-3}) and the probability of recovery is excellent ($1 - 2 \times 10^{-6}$).

Spacecraft charging as defined here refers to the buildup of charged particles and subsequent arcing on external spacecraft surfaces or on (and inside) internal surfaces. The former process is usually referred to as surface charging while the latter is termed internal charging. Since each process is associated with a different charged particle population, the details of the charging processes are somewhat different. To accommodate this difference, the two processes and their associated probabilities will be treated separately. As the principle effect of the two, namely, induced electrical transients, is similar, however, the final probability for failure due to spacecraft charging will be a combination of the two.

Although the outer surface of the Galileo spacecraft is designed to be an equipotential surface, some small surfaces will be electrically isolated by design or accident (see Galileo waiver list). Surface arcing, primarily near the Earth's geosynchronous orbit, could occur. Arcing can result in disruptive signals on the vehicle buss, damage to electrical devices, surface damage, and false signals. Arcing (likely due to internal charging rather than surface, however) is believed to have caused PORs on Voyager I and has been blamed for several serious spacecraft failures near the Earth.

Table A-25. Probability of Failure Due to Radiation-SEU Effects and Resulting in the Following ΔV During the Following Mission Phases

		$\lvert\Delta V\rvert = \lvert V_{nom}\rvert$
EGA - 60		
AXIAL+ Z	$0° < \theta < 30°$	
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1.7×10^{-5}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = 2×10^{-6}

EGA - 25		
AXIAL +Z	$0° < \theta < 30°$	
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1.7×10^{-5}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = 2×10^{-6}

EGA - 10		
AXIAL + Z	$0° < \theta < 30°$	
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1.7×10^{-5}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = 3×10^{-4}

Spacecraft surfaces will accumulate charge due to exposure to the space environment from the ambient plasma, sputtering, secondary emission, and photoelectron emission. As a rough estimate, the Galileo spacecraft could achieve potentials relative to space on the order of a few volts positive to several hundred volts negative in the solar wind and voltages as high as -20 kV near geosynchronous orbit at Earth. Only potential differences between surfaces, however, are of concern for arcing since a difference of 500 V or higher (depending on configuration) is necessary for a discharge to occur that could damage systems.

Data from the Earth-orbiting SCATHA spacecraft have clearly shown differential potentials on an electrically isolated test surface oscillating at 1 rpm by 2 kV as the surface rotated in and out of sunlight--more than sufficient to cause arcing. SCATHA is the most charging immune spacecraft ever flown yet it experienced approximately 147 discharges in 2.5 years of operations in and near geosynchronous orbit because of such potential variations. These arcs, as a function of amplitude, are presented in Figure A-23. As shown in Figure A-24, for an early portion of the mission, most of the arcs occurred in a narrow local time range between midnight and 03 LT. Interestingly, 28 of the 147 events occurred on 22 September 1982. Subtracting these 28 from the total implies that under normal conditions approximately 1 arc occurred every 7-8 days while, for exceptional geophysical conditions, the maximum rate could be as high as 1 or more per hour (approximately 1 day in 2.5 years). In contrast, a poorly designed spacecraft electrostatically, the geosynchronous TELECOM 1, had approximately 1 arc per day with the peak occurrence between noon and 18 LT. Thus arcing is quite common in and near geosynchronous orbit for even the most meticulously designed spacecraft and can occur at any local time dependent on the configuration of the spacecraft.

Unlike surface charging, which is typically in response to short term (hours to seconds) variations in the 10-100 keV electron environment, internal charging as a result of long term (months to years) exposure to the 0.1 - 1.0 MeV or greater electron environment can result in the buildup of electrons within dielectrics and on isolated conducting surfaces or wires inside the spacecraft. Briefly, electrons with energy in excess of 1 MeV can, unlike protons of the same energy, penetrate far into a surface before becoming trapped (see Figure A-25). These trapped charges build up in dielectrics or on internal conducting surfaces over long periods of time until the conditions for an arc breakdown occur (typical dielectric breakdown occurs for fields of 10E5-10E6 V/cm). In the case of Galileo, electrically isolated internal components, either dielectric or conducting, of the spacecraft may build up sufficient charge to cause arc breakdown. A random component may then arc causing false signals and/or part damage. The fact that the arc can occur internal to the electrostatic shielding makes this type of arc of particular concern.

As an example of internal charging, 42 anomalies on Voyager 1 were attributed to this problem during passage through the inner Jovian radiation belts. On Voyager 1, a sudden impulse, believed to be due to the internal charging and arcing, apparently stimulated a POR condition. In the case of Galileo, ungrounded wires (since corrected) were found to exhibit this behavior during ground testing.

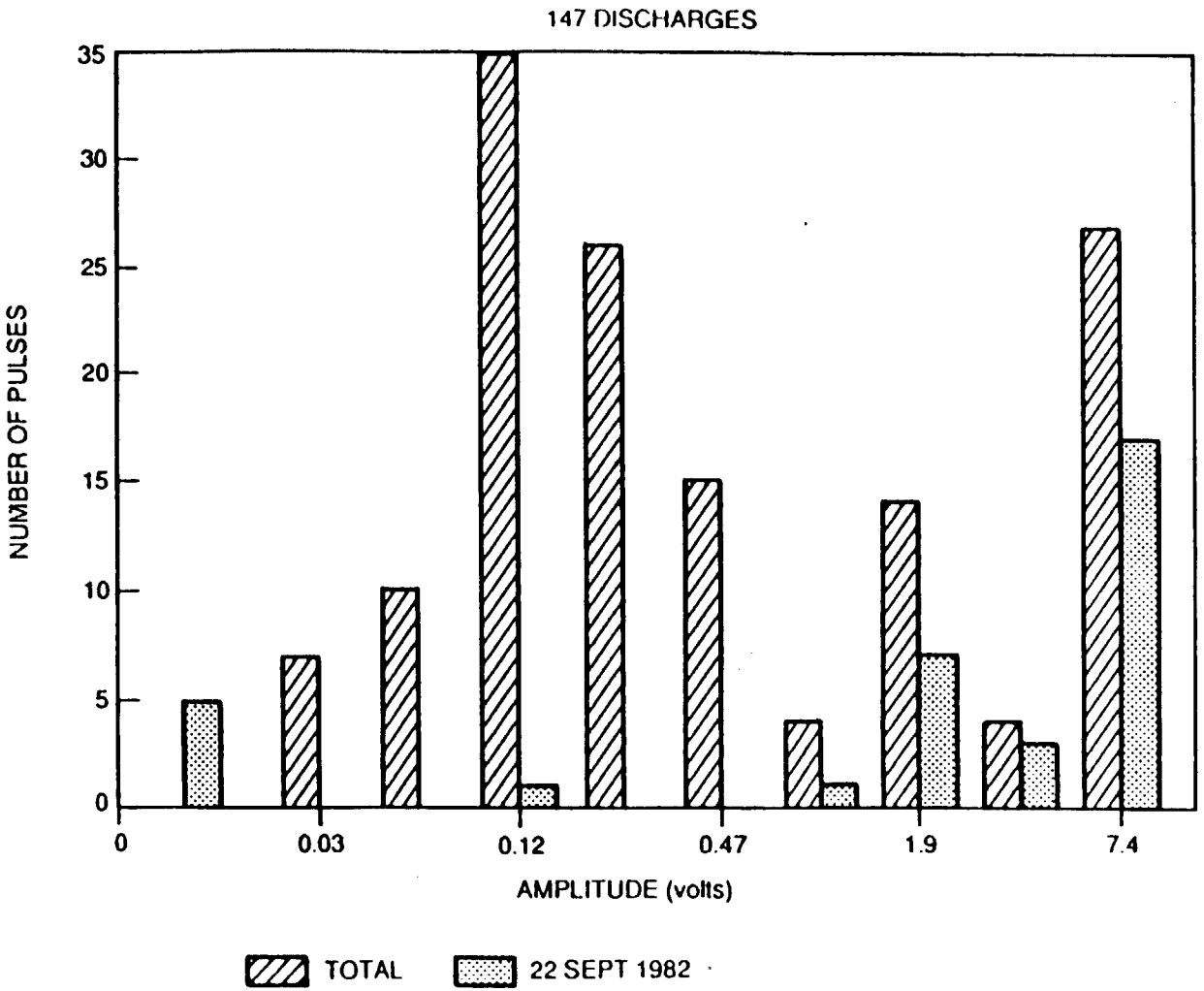


Figure A-23. Histogram of Arc Discharge Pulse Amplitude Distributions From SCATHA for the Period 1979 to 1982

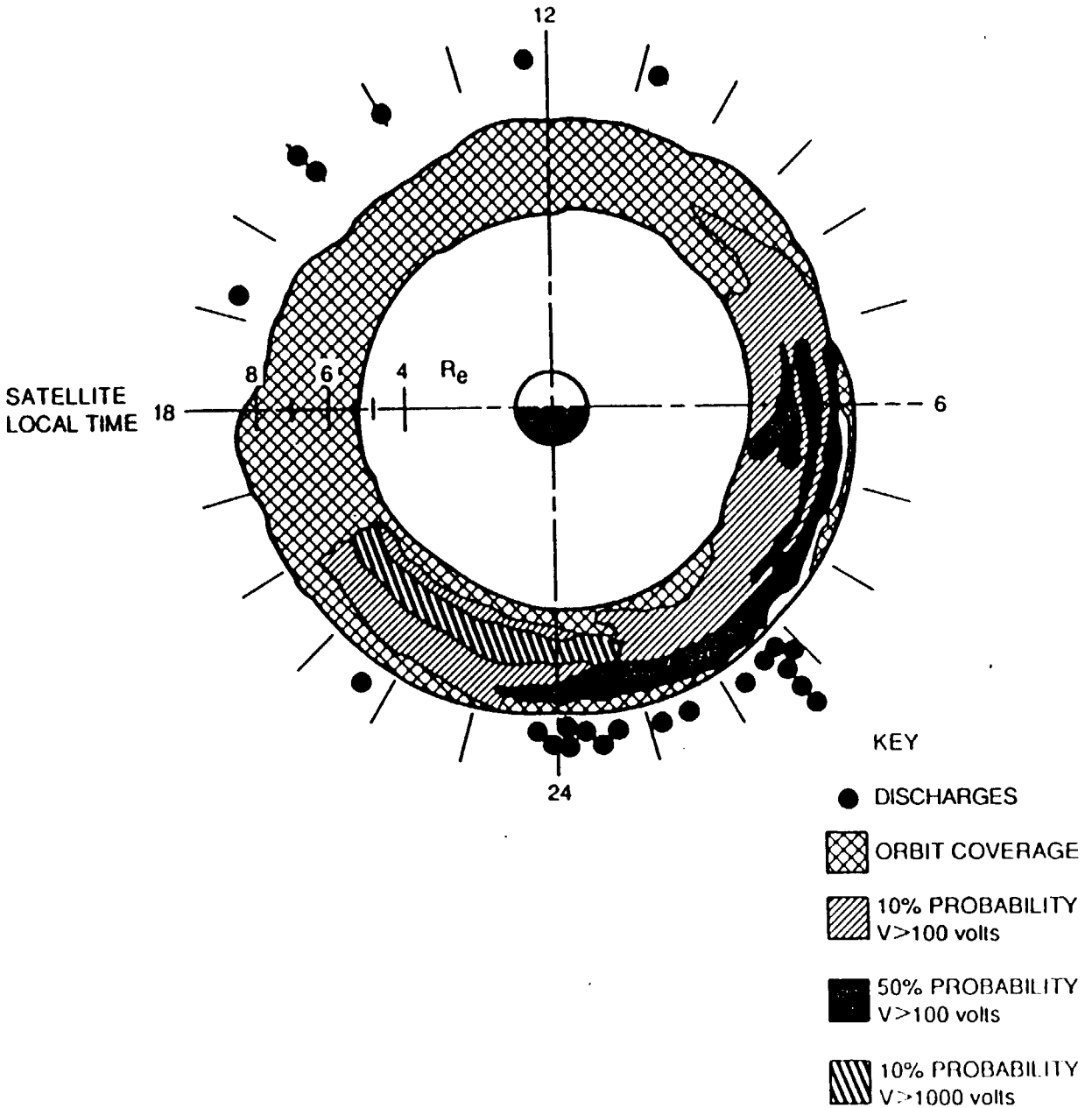


Figure A-24. Local Time Plot of the Occurrence of Arc Discharges and the Occurrence Frequency (in Local Time and Radius) of Charging Events From the SCATHA Spacecraft

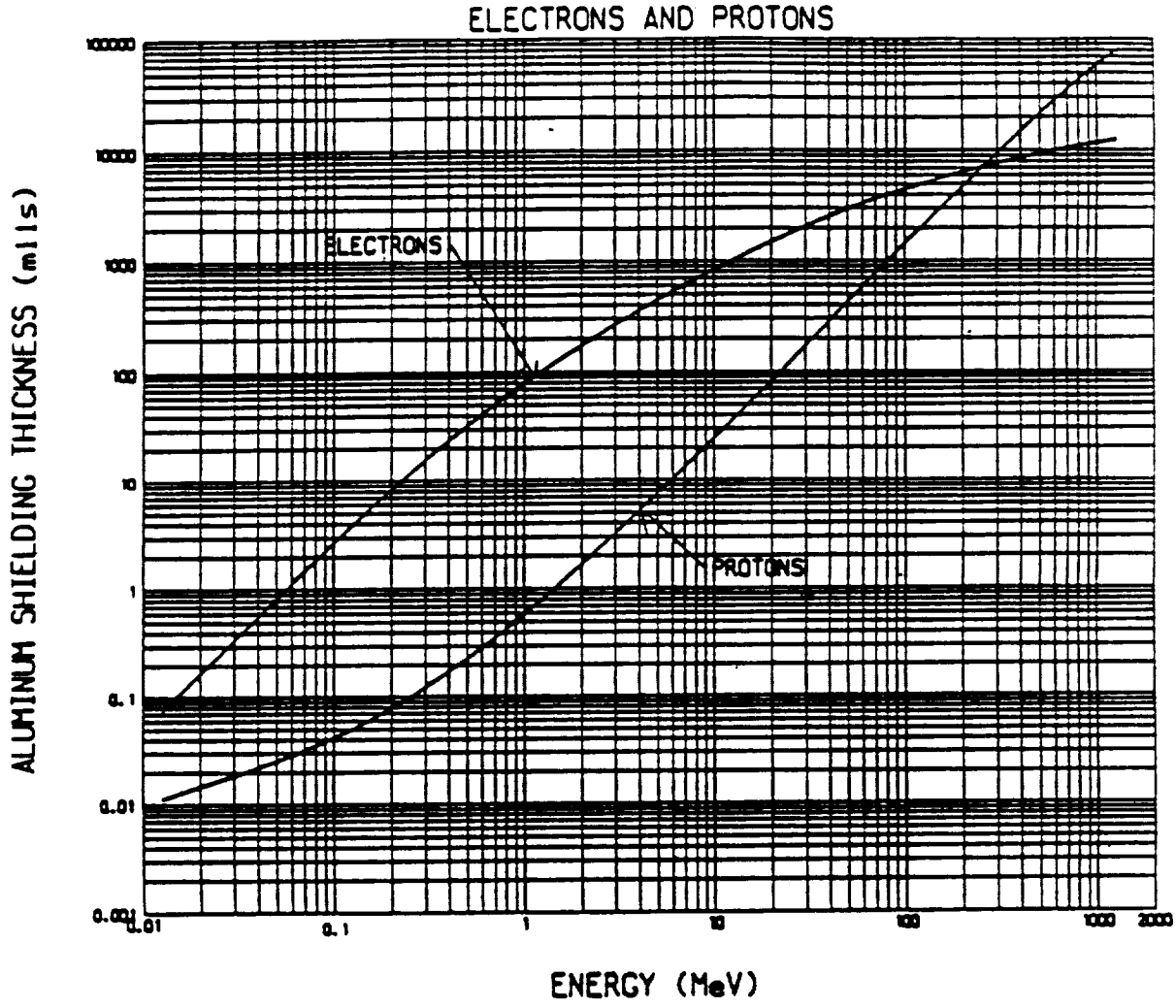


Figure A-25. Required Penetration Energy for Electrons and Protons Versus Shield Thickness

A.2.3.1 Probability Analysis for Failure. Although -100 V potentials have been observed in the solar wind, and anomalous conditions associated with a solar flare might produce higher potentials, it is unlikely that surface arcing is a concern in the interplanetary environment or near Venus. The main concern is within a few Earth radii of geosynchronous orbit and, in the absence of data on the actual Galileo response, likely to occur with equal probability at all local times. It will be assumed, therefore:

1) Probability of arc discharge in interplanetary space: 0.0

2) Probability of arc discharge during one Earth flyby:

   a) Arcs can occur uniformly between 5-10 Re and at all local times.

   b) Arc rate = 1 per 8 days = 1 per 192 hr (nominal-SCATHA)

      = 1 per day (poor design-TELECOM)

      = 1 per hr for 1 day in 900 (worst case-SCATHA)

   c) Susceptible period = 1 hr (Launch)

      2 hr (Flyby 1)

      2 hr (Flyby 2)

   d) Arc probability (from SCATHA data):

      0.5 V arc = 36/118 (nominal)

      = 64/147 (worst case)

      2.0 V arc = 18/118 (nominal)

      = 45/147 (worst case)

      7.5 V arc = 10/118 (nominal)

      = 27/147 (worst case)

   e) For Voyager, a 2 volt or higher arc on the line was required to cause upset. Assuming a similar level for Galileo as a conservative value (Galileo is better designed in this respect), the probability of one random IC upset per 2 hour transit (probability is 1/2 of these values for launch) is:

      Nominal probability for upset = (18/118) (2/192) = 0.15%
      Worst-case prob. for upset = (45/147) (2/900) = 0.068%
      "Poor design" prob. for upset = (18/118) (2/24) = 1.3%

(Note: The fact that a single day gave an anomalously large arcing rate may indicate a threshold effect for SCATHA arcing. This is probably spacecraft specific.)

The internal charging rate is a function of the existing charge (which complicates the local electric fields), the electrical properties of the material, shielding, and the incident flux. Although "pre-charging" of coaxial cables has been observed during the manufacturing process, it can be assumed that the vehicle is electrostatically "clean" to start with. Even given this assumption, the time to breakdown will be a complex convolution of the above variables so that the probability of breakdown can not be directly estimated. However, a "worst-case" estimate can be made. If the current in a typical arc is integrated over time, the total charge in an arc can be estimated to be on the order of about 1011 e- per event. Therefore, the earliest that sufficient charge could accumulate and cause an arc, based on Voyager and Galileo test experience, is when the total fluence exceeds 1011 e-/cm^2 since Galileo has been designed so that isolated, internal charge-collecting surfaces should not be larger than a few cm^2 (charge may bleed off, however, making this process rate dependent also). An arc would presumably deplete the accumulated charge so that a breakdown would likely not reoccur until the total fluence again exceeded 1011 e-/cm^2. The electron fluences (without shielding) above 0.1 MeV as a function of mission time are given in Table A-26 and those above 1 MeV in Table A-27. The 0.1 MeV (see Figure A-24) corresponds to the trapped charge expected near the surface while 1 MeV would correspond to the charge behind typical shielding. At the electron fluence rates expected for the VEEGA profile, the periods most critical for this effect are during the initial out-bound maneuver from Earth and during the two Earth flybys. In all cases, the region from about 2 Earth radii to about 8-9 Earth radii from the center of the Earth is the major contributor to total electron fluence until Galileo reaches Jupiter. Thus the greatest likelihood of arcing would be near the Earth as solar flares and the interplanetary environment do not contribute sufficient fluences of electrons.

At the levels of Tables A-26 and A-27, only an unshielded component very near the surface would likely experience internal charging since only the fluence at 0.1 MeV is sufficient to produce enough charge buildup over the time periods involved. A conservative estimate of internal arcing would be 100% probability for about 3 arcs on such an unshielded surface component during the first few hours following orbital injection, 4-7 during each of the two Earth flybys, and 0% during interplanetary transits. Given the careful design of Galileo, it is highly likely that any such arcs will be below the critical threshold for upset, but, as this cannot be known with certainty, it is conservatively assumed here that any arc will result in 1 upset.

A.2.3.2 Summary of Probability. The effects of surface charging can be summarized as follows. Barring the possibility of a design flaw (or "poor design") in Galileo, the total "nominal probability" value of 0.15% for the first Earth flyby is recommended as a conservative estimate of the arc discharge probability due to surface charging. As the only serious surface charging will take place near the Earth, when there is insufficient time to alter significantly the Earth relative trajectory, this effect would only affect the long range probability of impact on the return two years later. The difficulty of affecting the trajectory within 10 Re (Earth radii) of the Earth is discussed in Section 4.

Table A-26. Electron Integral Fluences Above 0.1 MeV for VEEGA 1989 Mission

Met	AE8MAX	Integral Fluence (/cm^2) Above 0.1 MeV	AE8MIN
0 - 107 min	3.18E11		1.52E11
0 - VFB SW		6.3E8	
VFB - EFB1 SW		1.2E9	
EFB1 (+ 70 min)	7.08E11		2.85E11
EFB2 - EFB2 SW		1.4E9	
EFB2 (+ 66 min)	3.85E11		1.80E11
EFB2 - JOI (.5.3 AU) SW		6.5E8	
TOTAL	1.4E12	3.9E9	6.2E11

AE8MAX corresponds to the model for electron fluxes at solar maximum, AE8MIN to those at solar minimum. VFB stands for Venus Flyby; EFB for Earth flyby; JOI for Jupiter orbit insertion; and SW for solar wind.

For internal charging, an arc will likely only occur during passage through the Earth's radiation belts. As a worst case estimate, a maximum of 7 internal arcs would be expected per flyby (much higher than the surface arcing rate). As in the case of surface charging, an arc during the actual orbital injection or the Earth flybys will be of minimal concern since it will be difficult for such errors to cause trajectory changes near the Earth which would lead to immediate impact (See Section 4). The only problem following such events would be long term effects on the subsequent Earth flyby. As another arc during the interplanetary phase will likely not occur, there should be sufficient time to recover from such an error.

Based on the preceding conclusion, the final probability of a ΔV due to spacecraft charging is estimated at 1.2×10^{-3}. This probability is arrived at in a similar fashion to the AACS memory chip failure calculation. Summarizing that development, it is argued first that only failures occurring outside the checksum region will be undetected and uncorrected. As there are 5376 bytes outside the total of 32768 bytes, this gives a probability of 0.16. A command resulting in an excess burn will be detected and corrected unless it is in the lateral direction. This limits the possibilities to the 1-3 m/s range and to a probability of 0.011 as there are only 60 bytes of the 5376 that could result in such an event.

Table A-27. Electron Integral Fluences Above 1 MeV for VEEGA 1989 Mission

Met	AE8MAX	Integral Fluence (/cm^2) Above 1 MeV	AE8MIN
0 - 107 min	9.11E9		6.23E9
0 - VFB			
SW		6.3E6	
CR		6.2E6	
VFB - EFB1			
SW		1.2E7	
CR		1.7E7	
EFB1 (+ 70 min)	1.15E10		7.86E9
EFB2 - EFB2			
SW		1.4E7	
CR		4.2E7	
EFB2 (+ 66 min)	9.10E9		6.21E9
EFB2 - JOI (.5.3 AU)			
SW		6.5E6	
CR		6.2E7	
TOTAL	2.97E10	1.7E8	2.03E10

Finally, there is a 0.1 probability that the bad bit will fail to be detected by the High Gain Antenna (HGA) correction algorithm. Thus, for 7 upsets (the surface charging arc probability is ignored):

$$\text{Prob} = 0.16 * 0.011 * 0.1 * 7 = 1.2 \times 10^{-3}$$

This is for a 1-3 m/s ΔV in the lateral direction. The probability of no recovery is taken to be 2×10^{-6} as it should normally be possible to recover from such an error (Table A-28).

A.3 GROUND INDUCED ERRORS

A.3.1 Command Generation

The Sequencing Process for generating and checking commands for the spacecraft was described in Section 2.3. The material presented here describes the most probable scenarios for errors to occur in that process. Command generation errors occur due to combined failure of automated software checks and procedural checks (human error).

These combined software and procedural checks will be discussed as a combined step, without specifying the detailed split between software and procedures unless necessary.

There are four ways to get an erroneous maneuver command to the spacecraft:

1) Send an erroneous individual maneuver command, instead of another command, or instead of no command. This category is further subdivided into the cases of sequenced commands and Real-time commands. The probabilities per day for such errors actually causing a ΔV to be implemented by the S/C are shown below to be 6×10^{-7} and 9×10^{-7}, respectively.

2) Send an erroneous value in any maneuver Profile Activity. Probability per Trajectory Correction Maneuver is shown to be 1×10^{-7}.

3) Send an erroneous maneuver PA instead of another PA, or instead of no PA. Probability is 6×10^{-11} per day.

4) Send an accurately built maneuver PA that reflects the Navigation Team's requested maneuver, but the Navigation Team has internally made an error. Probability per TCM is 2×10^{-4}.

In generating these scenarios, only the case where one erroneous command is sent, or one erroneous PA is sent is considered. Cases with multiple errors are considered even less probable. The exception to this is where Navigation erroneously requests an incorrect maneuver. To cover worst case situations, each error is assumed to be introduced as late as is possible in the Uplink Sequence Generation process, thus giving minimum opportunity for detection. The sequence checks are derived from the Galileo Space Flight Operations Plan (625-505, Vol. II, Operating Plans).

Table A-29 shows the possible ΔVs generated by these error scenarios. In each case anomalous velocity Ws are equally likely from zero to the specified maximum. Furthermore, all directions are equally likely, except as specified.

The individual command error is the case where a single command can cause the spacecraft to execute a ΔV causing maneuver. Three are of this type; an unbalanced turn command, a pulsed maneuver command, and a negative Z maneuver command. Since these commands can be sent either by placing them in the stored sequence or by sending them as a real-time command, this scenario is subdivided into those two subcases.

For the stored sequence route, the assumption of this report is that the error happens as late as possible in the Sequence Generation Process. For this scenario, the single command is inserted into the spacecraft stored sequence after the preliminary review, with the last updates to the sequence. From analysis of the Voyager Project experience in command errors[1], a

1 Error Management in Real-Time Commanding, IOM VOYAGER SCT-86-193, R. R. Lutz, 24 September 1986; and Error Management in Real-Time Commanding Status Update, IOM VOYAGER SCT-87-138, R. R. Lutz, 22 June 1987.

Table A-28. Probability of Failure Due to Spacecraft Charging and Resulting in the Following ΔV During the Following Mission Phases

		1 - 3 m/s
FIRST BURN AFTER EGA1		
AXIAL + Z	$0° < \theta < 30°$	
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1.2×10^{-3}
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = 2×10^{-6}

Table A-29. Maximum Erroneous Maneuver ΔVs

Error Class	Error	Max. ΔV (m/s) First three years in Mission
1) Erroneous Single CMD-Lateral		71.0
(7 BURN)	+Z	12.1
	-Z	57.8
(7 NEG Z)	-Z	6.0 (last value for 7AXDV)
(7 TURN)	Lateral	0.7
2) Erroneous Man. PA Value Any direction		5% high*
3) Erroneous Man. PA Any direction		345.5
4) Erroneous Nav Request Any direction		5**

*Time cutoff occurs at nominal value plus 5% maximum **1105.6 is the theoretical maximum, but based on analysis, any maneuver larger than 5 would be rejected.

probability of 6×10^{-2} (per day of sequence execution) is assigned to the possibility of introducing an erroneous command. This number is conservative in two distinctly different ways. First, the numbers for the Voyager Project included two spacecraft during most of the period, and second, Voyager did its sequencing primarily as individual commands.

Next consider the fact that only 3 commands are of concern. With a total of 1175 possible commands, a probability of 1×10^{-3} was assigned to the odds of the erroneous command being each of the 3 of concern (1/1175 rounded to 1 significant digit).

The next part in the process is a set of reviews of the sequence. These consist of two types of reviews. The first is a normal sequence review conducted by the Orbiter Engineering and Probe Engineering Teams. In this review, all of the individual commands in the sequence (as opposed to the PAs in the sequence) are scrutinized. Based on the presently perceived workload and engineering judgment, a probability of 5×10^{-2} was established for the likelihood that an erroneous command would slip through this check. A second check occurs where all of the commands of the type considered restricted (and all of these commands are) are separated out via software and individually reviewed by the same two teams. The same probability, 5×10^{-2}, was assigned to this review.

Then the sequence is presented to the Mission Director for approval. The purpose of this review is primarily to assure that all steps in the approval process have been properly followed. Therefore, it is considered unlikely that any erroneous commands would be caught in this step.

A command conference then occurs, where the sequence has been translated to the uplink command messages and final approval for sending those messages is given. Based on the format of the meeting and the review products available, it is unlikely that this would catch any erroneous commands.

At this point the commands are uplinked to the spacecraft and executed. No on-board checks would stop the execution of these individual commands. Table A-30 summarizes and totals the probabilities for this case. As a confidence check in these estimates, a comparison was made to Voyager experience. While Voyager did not send any erroneous maneuver commands, they have sent other commands in error. Voyager commands are subjected to steps 6, 9 (normal only, as all the Voyager errors were non-restricted commands), 10, and 11 in Table A-30, giving a probability of 3×10^{-3} per day, which agrees well with Voyager history.

The probability of recovery from an erroneous ΔV is a function of when the ΔV was performed with values as listed in Section 3.2.4.

For the real-time command route, the scenario is that the single command is inserted as either a restricted command request in the real-time command process, or is inserted as a request (erroneously) for a non-interactive command. Again from analysis of the Voyager Project experience in command errors, assume that on average there will be one command error per day. This number is also conservative in two distinctly different ways. First, the numbers for the Voyager Project included two spacecraft during most of the period, and second, Voyager sent many more real-time commands than Galileo will.

Table A-30. Sequence Checks in Process and Probabilities of Passing for Class 1A (Sequenced Individual Maneuver Command)

Step #*	Item	Probability per Execution Day
6	Introduce Erroneous Cmd	(6×10^{-2})
	Odds of it being one of 7BURN, 7NEGZ, or 7 TURN Commands	(1×10^{-3})
9	Flight Team Sequence Review - Normal	(5×10^{-2})
	Restricted Command	(5×10^{-2})
10	Flight Team Approval Meeting - Miss. Dir.	(1.0)
11	Command Conference	(1.0)
	Total Probability for each of 3 commands	(2×10^{-7})

* From Operating Plan Template and/or R/T CMD Process

Then take into account the fact that only three commands are of concern. A probability of 1×10^{-3} was assigned to the odds of the erroneous command being each of the three of concern.

The next part in the process is Command Planning and Integration performed by the Mission Control Team, where each command is reviewed for category (restricted, interactive, or non-interactive). Those commands deemed to be restricted or interactive are sent to the OET for the normal constraint sequenced commands. For those commands classified as non-interactive, only a review by the Mission Control Team and the Science Team requesting the command is performed. Based on engineering judgement, the probability of erroneously classifying a restricted command as a non-interactive command is 1×10^{-3}.

If these commands are correctly identified as restricted, the probabilities that the three commands of concern would be caught by the normal command review or the restricted command review are each 5×10^{-2}. The next part in the process is again a Command Planning Meeting run by the Mission Control Team, where the plans are set for when and how the commands are to be uplinked (no likelihood of catching a bad command). The next step is the Command Approval Meeting where the Mission Director gets a chance to review and approve all real-time commands. As these commands are never intentionally to be sent in real-time, the probability is 1×10^{-1} that the Mission Director will not catch this error. Then the commands are sent to the real-time operator and entered into the real-time command system to be uplinked to the spacecraft. No chance exists that this would catch a bad command.

If the command were erroneously classified as non-interactive, the command would have almost no chance of being caught in the Constraint Check by the MCT or Science Team. The next step, again, is the Command Approval Meeting where the probability is 1×10^{-1} that the Mission Director will not catch this error. Then the commands are given to the real-time operator, and entered into the real-time command system to be uplinked to the spacecraft. In this case, since the commands were erroneously classified as non-interactive, the command system will correctly notify the command operator that he is trying to send a restricted command. Since he must type in an override for this, the probability is 1×10^{-2} that the bad command will not be caught.

At this point the commands are uplinked to the spacecraft and executed. No on-board checks would stop the execution of these individual commands. Table A-31 summarizes and totals the probabilities for this case.

Again comparison to Voyager yields an expected rate of erroneous commands that proceed to execution in agreement with experience.

The erroneous maneuver PA value involves the case where a single error is made in the input to a planned maneuver PA. Since this is in the case of a planned maneuver, all probabilities are per Trajectory Correction Maneuver (TCM). Once again the assumption of this report is that the error happens as late as possible in the Sequence Process. The worst-case maneuver type planned for this period is the "fast response" type discussed in Section 3.2.4.3. From engineering judgment, assign a probability of 1×10^{-1} (per TCM) to the possibility of introducing the error. Then assign a probability to the error either affecting the direction of the TCM or magnitude (1×10^{-1}) instead of any of the other 18 PA parameters. Then further assign a probability to the error surviving software input checks on the PAs (1×10^{-1}).

Maneuver sequences are then further reviewed by an independent software check (the OET Maneuver Analysis Program Set, MAPS), which is assigned a probability of 1×10^{-3} for an error surviving the check.

The next part in the process is the set of reviews of the sequence. The first (normal sequence review) is assigned a probability of 1×10^{-1}. The second check (restricted sequence review) does not apply to PAs, but a different check for appropriateness of the PA for the applicable mission segment does. Since a maneuver was planned, 1.0 probability is assigned.

Then the sequence is presented to the Mission Director for approval. Based on engineering judgement, it is considered unlikely that any erroneous commands would be caught in this step.

A command conference then occurs, where the sequence has been translated to the uplink command messages, and final approval for sending those messages is given. Based on the format of the meeting and the review products available, it is unlikely that this would catch any erroneous commands.

Table A-31. Sequence Checks in Process and Probabilities of Passing for Class 1B (Real-time Individual Maneuver Command)

Item	Probability per Day	
Introduce Erroneous Cmd	1.0	
Odds of it being one of 7 BURN, 7 NEG Z, or 7 TURN Commands	1×10^{-3}	
Command Planning and Integration (MCT) Non-Interactive or Restricted	Interactive	
assigned as interactive or restricted	1.0	N/A
assigned erroneously as non-interactive	N/A	10^{-3}
Constraint Check/Risk Assessment (OET or MCT)		
Normal	5×10^{-2}	1.0
Restricted Command	5×10^{-2}	N/A
Command Planning Meeting (MCT)	1.0	N/A
Command Approval Meeting (Miss. Dir.)	10^{-1}	10^{-1}
Real-Time Command System Check	1.0	10^{-2}
Total Probability for each of 3 commands	3×10^{-7}	1×10^{-9}

At this point the commands are uplinked to the spacecraft and executed. No on-board checks would stop the execution of these commands. Table A-32 summarizes and totals the probabilities for this case.

Probability of recovery is dependent on how long before the Earth encounter the TCM is executed and uses the standard values described earlier.

The error where an erroneous maneuver PA is used involves the case where an entire unplanned maneuver PA is inserted into the sequence process. As this is an unplanned maneuver, all probabilities are per execution day. Once again the assumption of this report is that the error happens as late as possible in the Sequence Process. For this scenario, the error is inserted into the spacecraft stored sequence after the preliminary review, with the last updates to the sequence. From engineering judgement, assign a probability of 1×10^{-2} to the possibility of introducing the error. Then assign a probability to the error being one of the five PAs capable of causing a ΔV (6×10^{-2}).

Then comes the set of reviews of the sequence. The first (normal sequence review) is assigned a probability of 1×10^{-3} (as the reviewers have an excellent chance of detecting this problem). The second check (restricted sequence review) does not apply to PAs, but a different check for appropriateness of the PA for the applicable mission segment does. Since a maneuver was not planned, the probability is assigned as 1×10^{-3}.

Table A-32. Sequence Checks in Process and Probabilities of Passing for Class 2 (Erroneous Maneuver PA Value)

Step #	Item	Probability per TCM
3	Introduce Erroneous PA Value	10^{-1}
	Odds of it being in Direction or ΔV	10^{-1}
	Odds of it passing SEQGEN input checks	10^{-1}
	MAPS Check	1×10^{-3}
4	Flight Team Sequence Review - "Fast Response"	1×10^{-1}
	Restricted Command	N/A
	Mission Approval	1.0
5	Flight Team Approval Meeting - Miss. Dir.	1.0
9	Command Conference	1.0
	Total Probability	1×10^{-7}

Then the sequence is presented to the Mission Director for approval. Since these PAs are never intentionally to be sent as a part of a normal sequence, the probability is only 1×10^{-1} that the Mission Director will miss it.

A command conference then occurs, where the sequence has been translated to the uplink command messages, and final approval for sending those messages is given. Based on the format of the meeting and the review products available, it is unlikely that this would catch any erroneous commands.

At this point the commands are uplinked to the spacecraft and executed. No on-board checks would stop the execution of these commands. Table A-33 summarizes and totals the probabilities for this case.

In the case of a navigation design error, a single error is made in the input to a planned maneuver PA, but the error occurs in the Navigation design of the TCM, prior to the Sequence generation cycle. Since this is in the case of a planned maneuver, all probabilities are per Trajectory Correction Maneuver (TCM). From engineering judgement, assign a probability of 1×10^{-2} (per TCM) to the possibility of introducing the error in the ΔV vector determination step. Then assign a probability to the error surviving the independent maneuver verification step (2×10^{-2}). These represent very conservative estimates of error rates, since at the time of the final Earth delivery maneuvers, the Navigation Team will have had considerable experience in the design and verification of maneuvers.

Maneuver sequences are then further reviewed by an independent software check (the MAPS check), which is assigned a probability of 1.0 for this type of error surviving the check.

Table A-33. Sequence Checks in Process and Probabilities of Passing for Class 3 (Erroneous Maneuver PA)

Step #	Item	Probability per Execution Day
6	Introduce any Erroneous PA	10^{-2}
	Odds of it being a Man. PA	6×10^{-2}
9	Flight Team Sequence Review - Normal	10^{-3}
	Restricted Command	N/A
	Mission Approval	10^{-3}
10	Flight Team Approval Meeting - Miss. Dir.	10^{-1}
11	Command Conference	1.0
	Total Probability	6×10^{-11}

The next part in the process is the set of reviews of the sequence. The first (normal sequence review) is assigned a probability of 1.0, as the review would be verifying against the Navigation input. The second check (restricted sequence review) does not apply to PAs, but a different check for appropriateness of the PA for the applicable mission segment does. Since a maneuver was planned, the probability is assigned as 1.0.

Then the sequence is presented to the Mission Director for approval. Based on engineering judgement, it is cons commands. Table A-34 summarizes and totals the probabilities for this case.

The process described below specifically applies to the 7TURN will produce ΔVs only in the lateral direction (and is limited to changes of 0 to 0.7 mps). The last command, 7BURN, can produce velocity changes in both the -Z and lateral directions and along the +Z axis. Because the probability of an undesired 7BURN command is constant regardless of the direction in which it acts, its contribution to any one of the directions is 1/3 of its total probability.

Therefore, the probability of failure in each of the three directions was determined as:

in the +Z direction = 1/3*P(7BURN)
in the -Z direction = P(7NEGZ) + 1/3*P(7BURN)
in the lateral direction = P(7TURN) + 1/3*P(7BURN)

The probability of recovering from one of these errors is dependent on the time of the failure, including the recognition that there is a problem, and is described in Section 3.2.4.

Table A-34. Sequence Checks in Process and Probabilities of Passing for Class 4 (Navigation Design Error)

Step #	Item	Probability per TCM
2	Introduce Erroneous Nav Value	
	ΔV Vector Determination	10^{-2}
	ΔV Design Verification (Fast Response)	2×10^{-2}
4	Flight Team Sequence Review - Normal	1.0
	Restricted Command	N/A
	Mission Approval	1.0
5	Flight Team Approval Meeting - Mission Director	1.0
8	Command Conference	1.0
	Total Probability	2×10^{-4}

A.3.2 Uplink Transmission Errors

In this failure category, correct sequences undergo bit errors in transmission such that an erroneous but valid sequence is executed on board the spacecraft and it results in an anomalous velocity increment. For such a failure to occur, the following constraints apply:

Sequence bit flips are such that they escape the single error correcting, double error detecting uplink code. This requires 3 or more bit flips.

The uplink checksum must also remain correct. This requires an even number of bit flips and an unlikely coincidence.

Erroneous commands must appear valid to the AACS or other subsystem

Commands must result in an anomalous ΔV and inadequate ability to recover.

For such a failure to occur, there must be four or more bit flips in a command. With a bit error rate of 10^{-5}, the probability of this is 10^{-20} on a given command, or 10^{-17} per mission. In addition, it is unlikely that the command appears valid to the AACS and further unlikely that it results in an anomalous burn. Furthermore probability for recovery is excellent.

The resultant probability is less than 10^{-17} so this case will no longer be considered.

Table A-35. Probability of Failure Due to Erroneous Single Command, Sequenced, and Resulting in the Following ΔV During the Following Mission Phases

PROBABILITY PER DAY		0 → 0.7 m/s	0.7 → 6.0	6.0 → 12.1	12.1 → 71
AXIAL + Z	0° < θ < 30°	4×10^{-9}	4×10^{-8}	4×10^{-8}	0
MIXED	30° < θ < 60°	0 →	→	→	→
LATERAL	60° < θ < 120°	2×10^{-7}	7×10^{-9}	7×10^{-9}	6×10^{-8}
MIXED	120° < θ < 150°	0 →	→	→	→
AXIAL - Z	150° < θ < 180°	1×10^{-8}	2×10^{-7}	7×10^{-9}	6×10^{-8}

PROBABILITY OF NO RECOVERY = SEE SECTION 3.2.4

Table A-36. Probability of Failure Due to Erroneous Single Command, Real Time, and Resulting in the Following ΔV During the Following Mission Phases

PROBABILITY PER DAY		0 → 0.7 m/s	0.7 → 6.0	6.0 → 12.1	12.1 → 71
AXIAL + Z	0° < θ < 30°	6×10^{-9}	6×10^{-8}	6×10^{-8}	0
MIXED	30° < θ < 60°	0 →	→	→	→
LATERAL	60° < θ < 120°	3×10^{-7}	1×10^{-8}	1×10^{-8}	9×10^{-8}
MIXED	120° < θ < 150°	0 →	→	→	→
AXIAL - Z	150° < θ < 180°	2×10^{-8}	3×10^{-7}	1×10^{-8}	9×10^{-8}

PROBABILITY OF NO RECOVERY = SEE SECTION 3.2.4

Table A-37. Probability of Failure Due to Erroneous PA Value and Resulting in the Following ΔV During the Following Mission Phases

PROBABILITY PER TCM		0 - 5% HIGH
AXIAL + Z	$0° < \theta < 30°$	
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	1×10^{-7} *
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = SEE SECTION 3.2.4

* DISTRIBUTED EQUALLY OVER THE SPHERE

Table A-38. Probability of Failure Due to Erroneous PA and Resulting in the Following ΔV During the Following Mission Phases

PROBABILITY PER DAY		0 - 345 m/s
AXIAL + Z	$0° < \theta < 30°$	
MIXED	$30° < \theta < 60°$	
LATERAL	$60° < \theta < 120°$	6×10^{-11} *
MIXED	$120° < \theta < 150°$	
AXIAL - Z	$150° < \theta < 180°$	

PROBABILITY OF NO RECOVERY = SEE SECTION 3.2.4

* DISTRIBUTED EQUALLY OVER THE SPHERE

Table A-39. Probability of Failure Due to Navigational Design Error and Resulting in the Following ΔV During the Following Mission Phases

PROBABILITY PER TCM		0 - 5 m/s	5 - 1105 m/s
AXIAL + Z	$0° < \theta < 30°$		
MIXED	$30° < \theta < 60°$		
LATERAL	$60° < \theta < 120°$	2×10^{-4} *	~0
MIXED	$120° < \theta < 150°$		
AXIAL - Z	$150° < \theta < 180°$		

PROBABILITY OF NO RECOVERY = SEE SECTION 3.2.4

* DISTRIBUTED EQUALLY OVER THE SPHERE

A.4 PROBABILITY OF RECOVERY

A detailed evaluation is developed here for the probability of the spacecraft being able to recover from an anomalous ΔV, given that the initial failure does not interfere with the recovery. This probability is a function only of the time of the initial failure. There are several limiting factors, the importance of which depends on this time. The limiting factors are:

1) A subsequent dual failure in the spacecraft which prevents further recovery operations.

2) A subsequent single failure in the spacecraft which aborts the first recovery attempt, perhaps leaving insufficient time for further recovery attempts.

3) An error made in the process of developing the recovery maneuver on the ground. By the time the error is discovered, there may be insufficient time to attempt another recovery maneuver.

4) The initial failure may occur so close to Earth flyby that there is insufficient time to plan and execute a normal recovery maneuver. A maneuver developed in a quick turnaround mode is more likely to be in error.

Table A-40 presents a summary of these recovery failure categories, their relevant time domains and the associated probability of no recovery. The following paragraphs explain how the probabilities were determined in each case.

A.4.1 Two Spacecraft Hardware Faults

Typically it will take two spacecraft faults to result in the initial failure which imparts a ΔV to the spacecraft. For most such failures, there is a good chance of effecting a recovery maneuver if in fact one is required in order to avoid the Earth. If there is plenty of time to execute the recovery maneuver (more than 20 days), then it will take two more faults to cause a recovery failure. The first of these, which could have occurred any time in the mission up to the time of the recovery maneuver, would abort the first recovery attempt in the first 10 days after the failures that caused the ΔV. The second would abort a second recovery attempt on redundant systems performed in the next 10 days.

There have been determined to be approximately 10 such two fault cases which would prevent a non-time-constrained recovery. In each case, the first fault must happen sometime in the first three years of the mission to be in effect at the time of flyby. The probability of such a first fault is:

$$(10 \text{ failure modes}) \times \frac{3 \text{ years}}{(1 \text{ Mission})} \times 10^{-2} \cong 1/30$$

The second fault must occur sometime in the 20 days following the initial failure which resulted in the ΔV. If it had happened earlier than this, two spacecraft disabling faults would already be in effect in redundant systems at the time of the initial failure. The spacecraft would be inoperable, the mission would be over, and no maneuvers or other spacecraft activity would be taking place which could have resulted in the failure causing the ΔV. If the second fault occurred after the 20 days following the initial failure, the recovery would have already been achieved. Therefore the probability of the second fault is:

$$\frac{(20 \text{ days})}{1 \text{ Mission}} \times 10^{-2} = 6 \times 10^{-5}$$

and the probability of two hardware failures preventing recovery is

$$1/30 \times 6 \times 10^{-5} = 2 \times 10^{-6}$$

for all initial failures which occur more than 20 days before an Earth flyby.

A.4.2 One Spacecraft Hardware Fault

If the initial spacecraft failure which results in a ΔV occurs sufficiently close to the flyby, it is possible for a single hardware fault to prevent recovery. Specifically, if the initial failure occurs between 20 and 10 days before flyby, there will, conservatively, only be adequate time for a single recovery attempt, and several single faults can prevent the recovery. There have been determined also to be approximately 10 such hardware faults which will prevent recovery in these 10 days. The probability of interference from such faults is

$$(10 \text{ failure modes}) \times \frac{10 \text{ days}}{1 \text{ mission}} \times 10^{-2} = 3 \times 10^{-4}$$

A.4.3 One Ground Error

All maneuvers, including recovery maneuvers, are generated on one of three timelines, the Standard Response, the Fast Response, and the Time Critical Response. These take ten, six, and three days, respectively to generate and send to the spacecraft. Subsequently, approximately two more days are needed to determine whether the maneuver was successful and determine the new spacecraft trajectory. Based on the analysis presented in Section A.3, the probability of errors in each of these response modes in 1×10^{-4}, 2×10^{-4}, and 5×10^{-3}, respectively.

It is planned that recovery of the spacecraft, when required less than ten days from Earth, would be done with successive maneuvers of the Time Critical Response type until one is successful. Ground errors will become the limiting factor in recovery when there is only time for a single recovery attempt. Therefore for initial failures which occur between 3-1/2 and 10 days before Earth closest approach, the probability of no recovery is bounded by 5×10^{-3}, and will be reduced below this value when time for more than one attempt is available. In keeping with the conservative philosophy of this analysis, 5×10^{-3} will be used for these cases.

A.4.4 One "Quick" Ground Error

When there is insufficient time for a recovery maneuver which is subjected to all normal checks, but there is adequate time to generate and send a maneuver using standard maneuver profile activities, the probability of a successful recovery is 0.9. This will be the case from 3-1/2 to 1 day before Earth flyby.

A.4.5 One "Emergency" Ground Error

When there is only time to send a few commands to the spacecraft with only minimal checking, the probability of recovery is taken to be only 0.1. This will be the case for the last day before Earth flyby.

A.4.6 Use of Recovery Probabilities

For the detailed fault category recoveries analyzed previously in this Appendix where the standard recovery probabilities are applicable, the values summarized in Table A-40 are used. These probabilities only apply where the initial fault does not interfere with the recovery.

Table A-40. Probability of No Recovery

	Time of Failure Before Encounter (days)	Limiting Factor on Recovery	Probability of No Recovery
1.	20 or more	2 S/C H/W Faults	2×10^{-6}
2.	10 to 20	1 S/C H/W Fault	3×10^{-4}
3.	3-1/2 to 10	1 Ground Error	5×10^{-3}
4.	1 to 3-1/2	1 "Quick" Ground Error	0.1
5.	8 hrs to 1	1 "Emergency" Ground Error	0.9