

Enhancing the Cassini Mission through FP Applications after Launch

Paula S. Morgan
Jet Propulsion Laboratory/California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109-8099
818-393-1092
Paula.S.Morgan@jpl.nasa.gov

Abstract— Although rigorous pre-emptive measures are taken to preclude failures and anomalous conditions from occurring in JPL spacecraft missions prior to launch, unforeseeable problems can still surface after liftoff. In the case of the Cassini/Huygens Mission-to-Saturn spacecraft, several problems were observed post-launch: 1) immediately after takeoff, the collected engineering/science data stored on the Solid State Recorders (SSR) contained a significantly higher number of corrupted bits than was expected (considerably over spec) due to human error in the memory mapping of these devices, 2) numerous Solid State Power Switches (SSPS) sporadically tripped off throughout the mission due to cosmic ray bombardment from the unique space environment, and 3) false assumptions in the pressure regulator design in combination with missing heritage test data led to inaccurate design conclusions, causing the issuance of two waivers for the regulator to close properly (a potentially mission catastrophic single-point failure which occurred 24 days after launch) - amongst other problems. For Cassini, some of these anomalies led to arduous work-arounds or required continuous monitoring of telemetry variables by the ground-based Spacecraft Operations Flight Support (SOFS) team in order to detect and fix fault occurrences as they happened. Fortunately, sufficient funding and schedule margin allowed several Fault Protection (FP) solutions to be implemented into post-launch Flight Software (FSW) uploads to help resolve these issues

autonomously, reducing SOFS ground support efforts while improving anomaly recovery time in order to preserve maximum science capture. This paper details the FP applications used to resolve the above issues as well as to optimize solutions for several other problems experienced by the Cassini spacecraft during its flight, in order to enhance the spacecraft's overall mission success throughout the 18 years of its 20 year expedition to and within the Saturnian system.¹

TABLE OF CONTENTS

1. INTRODUCTION	1
2. PRE-LAUNCH: ENSURING MISSION SUCCESS .3	
3. AT LAUNCH: HIGH SSR BIT FLIP COUNTS6	
4. L+3WKS: REGULATOR MALFUNCTION	8
5. L+4MOS: SPURIOUS SSPS TRIPS.....	12
6. SATURN-4 YRS: PROBE RELAY ERROR	14
7. SATURN-3 YRS: POOR S/C=> EARTH LINK..	15
8. IMPLICATIONS FOR CASSINI'S EOM	17
9. CONCLUSIONS & LESSONS LEARNED	18
ACKNOWLEDGEMENTS	18
REFERENCES	18
BIOGRAPHY	19

1. INTRODUCTION

The “Class A” Cassini/Huygens Mission-to-Saturn spacecraft was launched on October 15, 1997 to investigate the Saturnian system (Figure 1); that which offers a rich environment for scientific study and exploration. Saturn's elaborate ring system serves as a physical model for the disc of dust and gas that once surrounded our early Sun, from which the planets were formed. The successful search for other planetary systems elsewhere in our galaxy is supported by projects such as Cassini, since the early stages of planet formation can be understood by observing Saturn's dynamic system. Currently, missions like the Kepler Telescope Spacecraft which endeavor to seek out habitable planets, are built upon discoveries like those from the Cassini mission, which aid in our understanding of planetary system architecture.

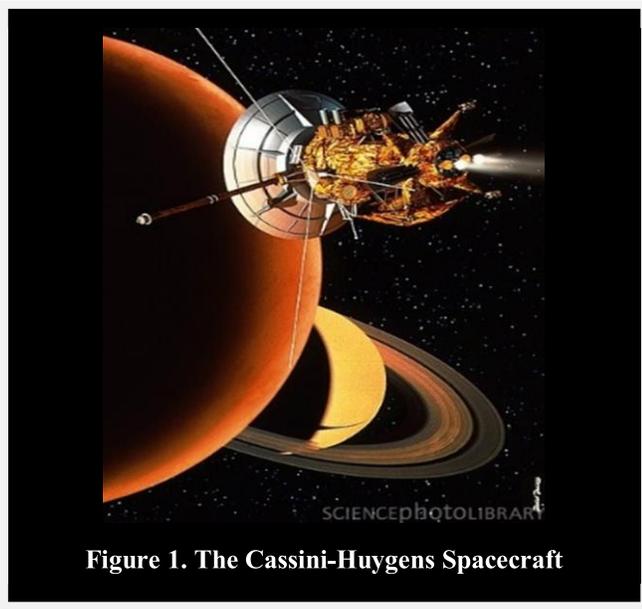
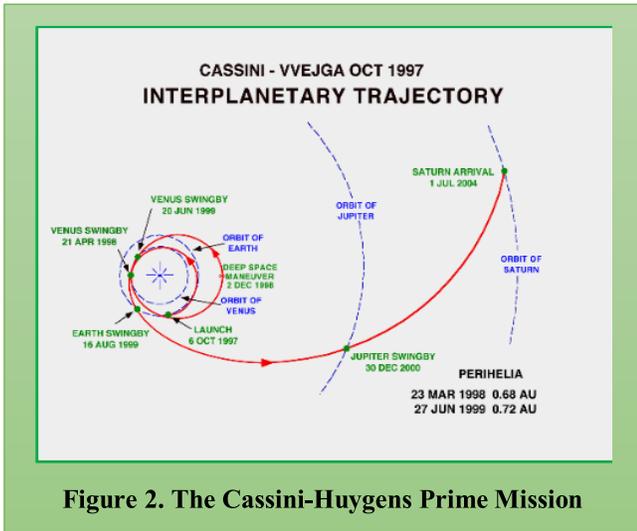


Figure 1. The Cassini-Huygens Spacecraft

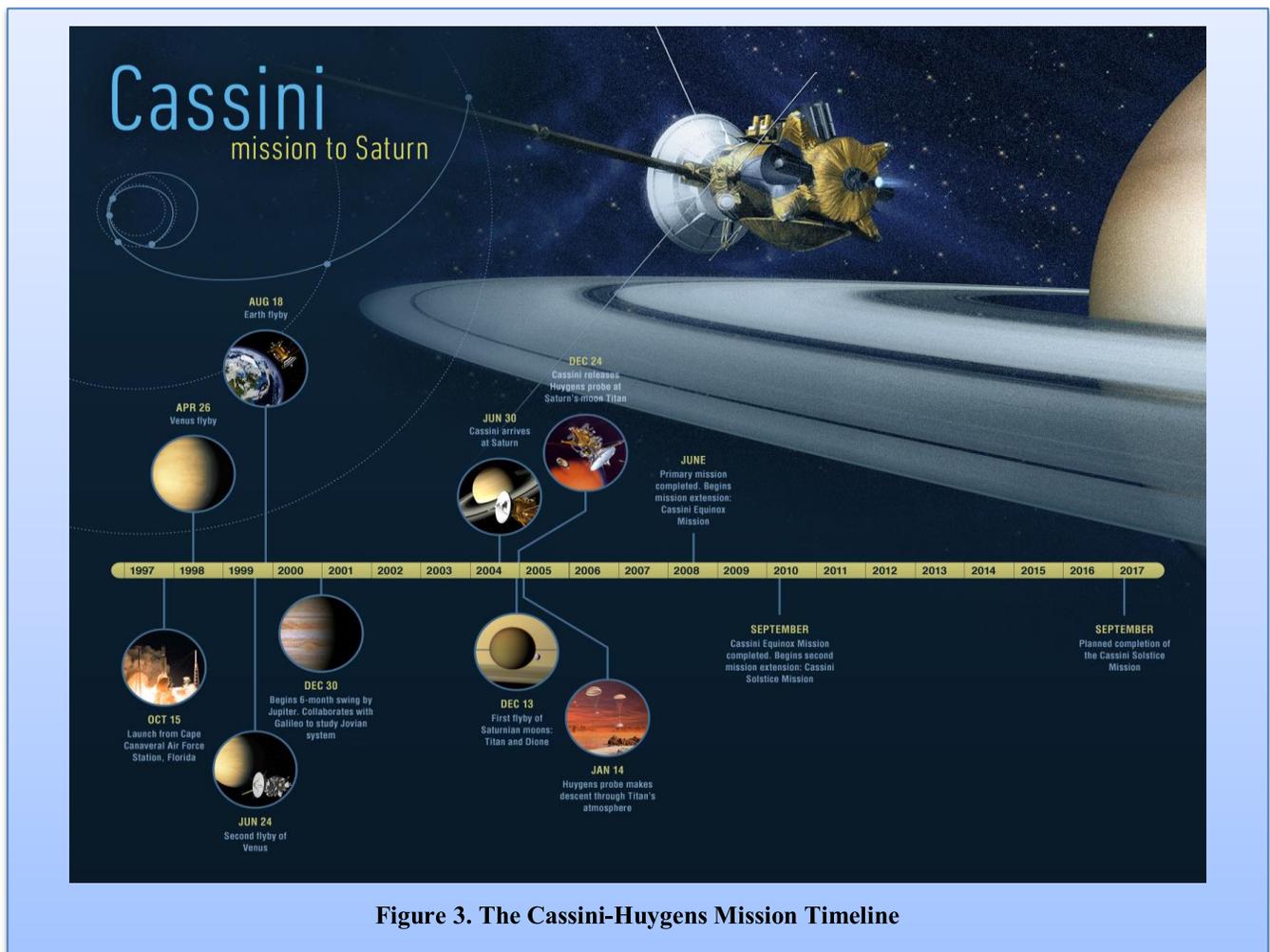
¹ 978-1-4673-7676-1/16/\$31.00 ©2016 IEEE

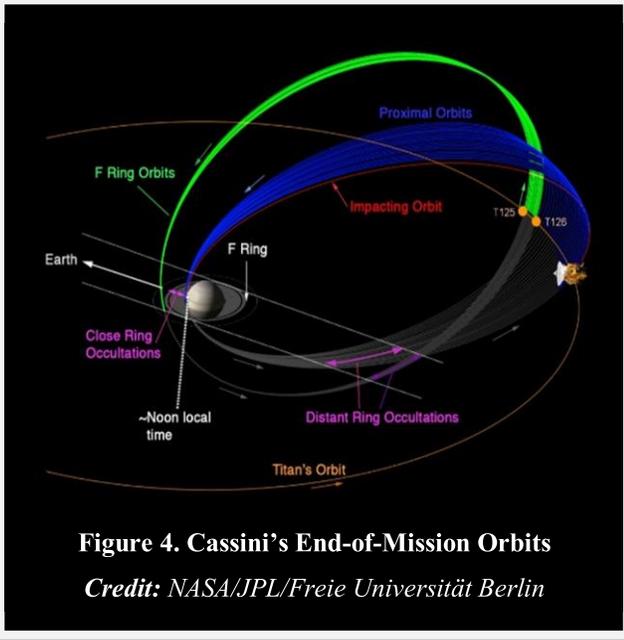


In the past, flybys of Saturn were made by Pioneer 11 (1979), Voyager 1 (1980), and Voyager 2 (1981); missions which led to plans for Cassini's encounter at Saturn, starting in 1982. To date, the Cassini-Huygens mission has provided detailed knowledge of the history and processes occurring on the planet's diverse moons, captured valuable data on chemical, geologic, and atmospheric processes as well as providing

knowledge about Saturn's magnetosphere and ring system. Investigation of the Titan moon was carried out by the Huygens Probe, examining its atmospheric conditions, wind characteristics, temperature information, and surface state; all of which is of special interest to scientists, since Titan is the most Earth-like moon in our solar system [1].

The Cassini-Huygens Program is an international science mission with 3 main participants (Jet Propulsion Laboratory, the European Space Agency, and the Italian Space Agency) as well as 17 nations, all who partook in the design and construction of the Cassini spacecraft, its instrument suite, and the Huygens Probe. The mission profile called for a 6.7 year cruise to the Saturnian system by way of 4 planet-assist flybys (Venus-1, Venus-2, Earth, and Jupiter), a descent into Titan's atmosphere by the Huygens Probe once reaching the Saturnian system, and a 4 year Prime Tour of Cassini orbiting Saturn & Titan in order to survey the planet's system until 2008 (Figure 2). A 2-year extension of the mission was granted by NASA (called "The Equinox Tour"), with a second extension (from 2010-2017) called "The Solstice Tour." The mission will end in 2017 with "The Grand Finale" where very fast orbits around the outer F-Ring & innermost D-Ring will be followed by a fiery plunge into Saturn (Figure 3 & 4).





Cassini Spacecraft & Instrument Configuration: The 3-axis stabilized Cassini spacecraft is the largest outer planetary explorer ever built, consisting of 12 scientific instruments configured to perform a wide variety of science observations on a multitude of designated targets. The Huygens Probe has 6 instruments of its own, and its goals are to investigate Titan's environment and surface characteristics. Cassini's science objectives at Saturn consist of examining the planet's atmospheric properties and composition, internal structure, rotation rate, ionosphere, as well as ring composition and its dynamic processes, and interactions with the many moons which surround this dusty environment [2]. Cassini's 3 Radioisotope Thermoelectric Generators produce power for the 192 SSPS switches aboard the spacecraft. Two Command and Data System (CDS) IBM 1750A computers (512K RAM) contain redundant 1553 Busses which receive and process "real-time" and "sequenced" ground commands for the spacecraft's engineering subsystems and science instruments to execute. CDS stores computer & instrument Flight Software (FSW) loads (and stores collected science & engineering data for later downlink) on two TRW designed SSRs (2.5Gb total storage capacity/per SSR with 2.1Gb usable for data, containing 640 Dynamic Random Access Memory units; DRAMs). Two Attitude & Articulation Control System computers (AACS) provide attitude determination using stellar reference units via a 3,500 on-board star catalog, where attitude and vehicle body rates are supplied by Hemispheric Resonator Gyros (internal reference units), and 3-axis stabilization is provided by Reaction Control System (RCS) thrusters or 3 reaction wheels. Cassini's Propulsion Maneuvering System (PMS) consists of redundant Main Engines (ME) which use a bipropellant configuration consisting of Monomethyl Hydrazine and Nitrogen Tetroxide hypergolic fuel & oxidizer propellants, and a monopropellant (Hydrazine) RCS system with 16 redundant thrusters. The telecommunications system consists

of one 4-meter High Gain Antenna (HGA) which is used for main communications (as well as to shade the spacecraft components from sun exposure during inner solar system cruise), and two Low Gain Antennas (LGA) which are primarily used for emergency communications in anomaly situations. Redundant Deep Space Transponders (DST) receive uplink signals (commands) from the Deep Space Network (DSN) ground stations, while an on-board Ultra Stable Oscillator (USO) provides 1-way doppler downlink, then 2-way coherent doppler through the DST's Voltage Controlled Oscillator (VCO). Redundant 20 Watt Traveling Wave Tube Amplifiers (TWTA) are also used in the downlink path of the Radio Frequency System (RFS). The thermal protection system consists of passive components such as blanketing & surface treatments, radioisotope heater units, and instrument radiators that face the cold region of space. Active thermal protection components consist of louvers, Autonomous Thermal Control (ATC) of selected components and replacement & supplemental heaters are used to protect the instruments in order to avoid damage to these devices. [3].

2. PRE-LAUNCH: ENSURING MISSION SUCCESS

Before launch approval could be obtained for Cassini, numerous analyses & tests had to be performed and approval obtained by NASA to assure Cassini's flight worthiness. Cassini is a "Class A" Flagship mission which requires that it be configured as a low risk tolerance/high robustness design with all practical measures taken to assure mission success. A strategy for single fault tolerance must be employed with the possible implementation of a multiple fault tolerance design. NASA requires that no single permanent hardware (HW) fault or one or more non-simultaneous single recoverable faults shall cause a loss of the mission. Any exceptions shall be separately exempted from this Single Point Failure (SPF) list via Project Management approval. The spacecraft must have the ability to "fail operational" for any SPF fault that occurs, with the stipulation that it respond to any failure in a timely fashion (before mission objectives are irrevocably compromised or non-recoverable damage is done). For Cassini, the spacecraft must be able to survive any failure without Spacecraft Operations Flight Support (SOFS) ground assistance for 2 weeks, and must have HW & SW fault containment regions to prevent a single fault from impacting the spacecraft's critical functionality or preventing the use of multiple units or subsystems. In all cases, the SOFS team of engineers is responsible for failure diagnosis (using telemetered parameters) and recovery from all fault conditions.

Analyses & Testing: To comply with these NASA standards, numerous pre-launch analyses and test programs were performed to fulfill all mission requirements. A spacecraft loads analysis was conducted to demonstrate that all structural margins met expected safety standards; an assessment which was precluded by a modal test program that yielded experimental data to verify the spacecraft and instruments, via a finite element model arranged in the launch configuration. Dynamic testing of the spacecraft and

Table 1. Mission & Systems Definition Process

SPACECRAFT DEVELOPMENT LIFE CYCLE: MISSION CONCEPTION THROUGH OPERATIONS						
NASA Phases =>	FORMULATION			IMPLEMENTATION		
JPL Life Cycle Phases =>	Pre-Phase A: Advanced Studies	Phase A: Mission & Systems Definition	Phase B: Preliminary Design	Phase C: Detailed Design	Phase D: Build & Test	Phase E: Operations
			Product Implementation Plan (Work Agreements)	Operations Plans	Operations Procedures	Engineer & Science Subsequences
					Block Dictionary	Real-Time Commands
					Operation Interface Agreements	Subsystem Reports
					Software Interface Specifications	Sequence Predicts & Alarms
						Engineering Change Requests
						Archived Products
						Anomaly Resolution Products

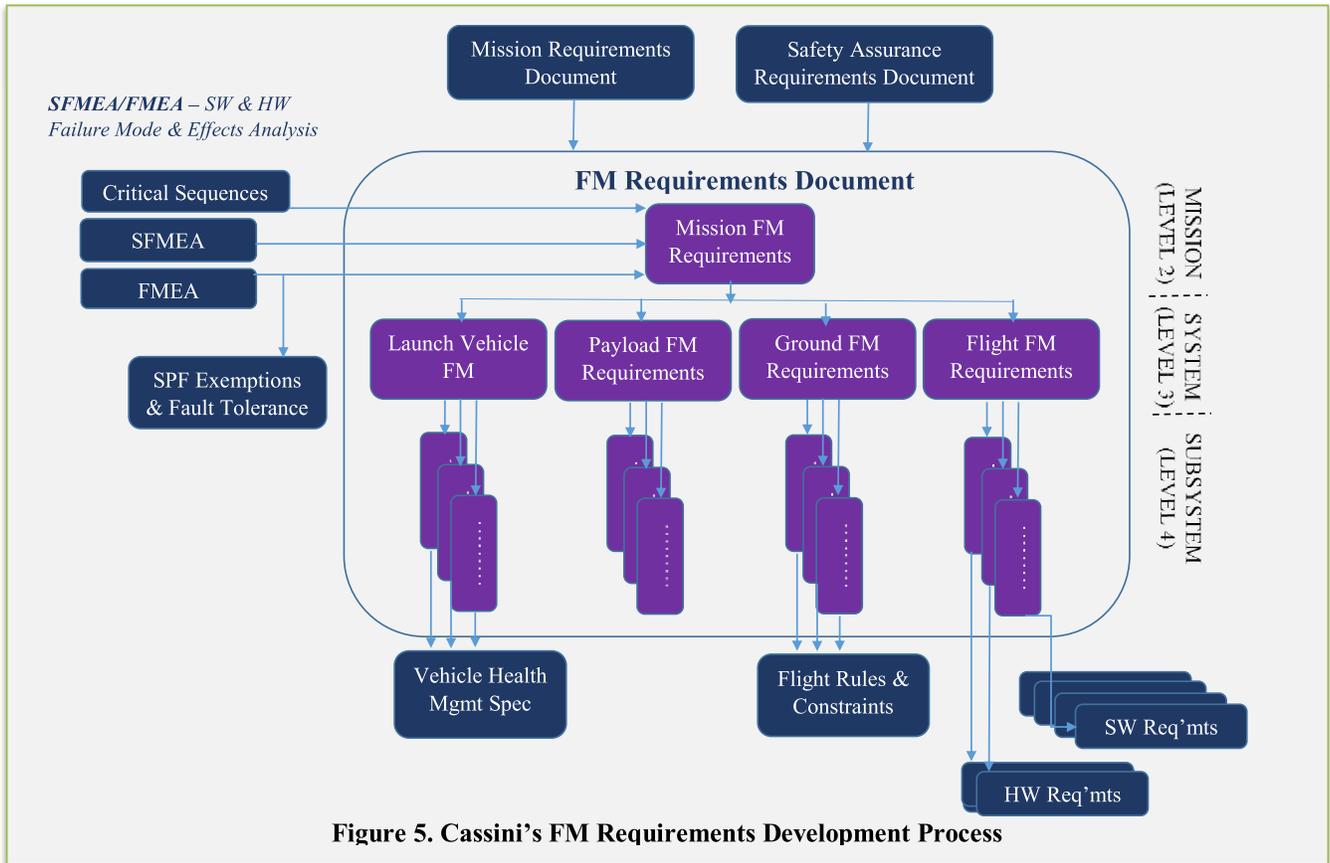
instruments was also performed, along with acoustic/vibration tests [4, 5, 6, & 7]. Thermal analyses provided environmental verification, proving the functionality of all components, and verification of heater power and the radiator area for engineering subsystems, as well as transducer performance verification [8 & 9]. Thermal blankets applied to Cassini’s exterior provided not only thermal protection from the sun’s heat and the deep cold of space, but also ensured no damage from meteoroid impact [10].

In addition to these rigorous HW test programs, fault preventative measures must also be implemented into Cassini’s FSW. Once launched, Cassini’s external and internal systems must be continuously monitored, regulated, and controlled. Fault Protection (FP) techniques are implemented to ensure that the health and safety of the vehicle is maintained throughout its mission. Of additional concern is the ever increasing lag time where the earth-spacecraft distance grows as the spacecraft approaches Saturn (called “round trip light time;” RTLTL), which becomes a high risk deterrent to fault recovery for some fault conditions should they occur. In these cases, it can be impossible to fix the fault via SOFS ground commanding in time to avoid a catastrophic failure (e.g. a leaking regulator which allows pressurant to fill the fuel tank leading to tank rupture). Therefore, autonomous FP routines are needed to monitor spacecraft systems and autonomously respond to anomalous conditions through “canned” automated responses that can facilitate redundant unit swaps and/or place the spacecraft in a safe state using preprogrammed instructional routines [11]. To achieve this goal, Fault Management (FM) techniques were implemented early in Cassini’s design phase.

FM Development & Implementation: FM implementation begins in Phase A during the Mission & Systems Definition stage (Table 1). FM requirements for the mission are derived from Mission Requirements generated during the proposal phase (including Safety & Mission Assurance Requirements). The resulting FM requirements are captured in documents as a set of clear and concise mission-level engineering requirements which are eventually allocated to the ground systems and mission operations teams. The development of all requirements is an iterative process which is performed simultaneously with (and is dependent on) the development of the mission technical concept, the FM concept, and the fault tolerance, safety, & reliability requirements. They are developed and refined by using the output of scenario analysis, operational mode development, and fault analyses, using mission science & engineering trade studies. These analyses are performed from Phase A and refined throughout Phases B & C. The series of mission-level FM requirements are formulated, yielding numerous external documents for the SOFS subsystem teams to follow, listing FP areas of responsibility, potentially bad conditions, and the principles of FM architecture (which were developed in Phase A; Figure 5). Once the mission-level FM requirements are developed, they are further broken down and allocated to the various systems (Level 3), and then allocated to the subsystems (Level 4).

The FM Design Specifications & Design Documentation is written to specify detailed descriptions and diagrams of failure detection monitors and corrective action responses including assumptions, failure potential, algorithm prioritization, and interaction prevention logic. It also contains the Safe-Mode (Safing) Response design description, with failure detection, isolation, and recovery algorithms, time critical sequences, and ground interaction requirements. Details of the overall operations scenario which describe end-to-end operation of the system after launch is also included, specifying operational phases, payload (instrument) operations & observations, data management, and other aspects of the day-to-day execution of the mission.

FSW Verification & Validation: The Verification & Validation (V&V) effort starts in Phase B and continues through Phase D where the FM Requirements are thoroughly tested in FSW. Simulators and “test-beds” are utilized for certification and configured to the required fidelity, focusing on the core functionality of the system through realistic scenarios performed at the highest level of integration possible. This process defined the agreement between Project Management with FM on the list of tests which must be completed successfully prior to the launch. Discrepancies in the test output are documented in Problem Failure Reports (PFRs) which are in turn fixed in FSW and then retested. For Cassini, late FSW deliveries (which in turn delayed testing) required that high priority PFRs be fixed pre-launch and retested, with low risk items deferred until after launch (to be uplinked to the spacecraft in planned future FSW uploads). But pre-launch, all identified SPFs were accounted for and



tested successfully in the FM design, with the exception of those class of faults which were identified to be placed on the “SPF Exempt List” list (Table 2). For projects like Cassini which contain redundant systems, this SPF Exemption List defines the agreement between Project Management and FM on a list of system components for which no FM will be applied. ANY violation of this SPF Exemptions List requires a project waiver with thorough justification if it be a Class A mission like Cassini [12].

Exempted Failures: The Cassini Project policy calls for a strategy which precludes all SPFs, stating that “No credible single point failure shall prevent attainment of mission objectives or result in a significantly degraded mission, with the exception of those failure exemptions listed in the Cassini Single Point Failure Exemptions List.” These objectives preserve the ability to obtain minimum essential engineering data and command capability needed to operate the spacecraft, the completion of a successful earth swingby, spacecraft targeting, successful Saturn Orbit Insertion (SOI), delivery of the Huygens Probe to Titan with data return, and acquisition of science data from all except one instrument, or the acquisition of the minimum engineering data needed to interpret the science data from all except one instrument. Mission degradation is considered “significant” if either a viable mission exists but most of the primary mission objectives cannot be met, or a satisfactory mission can be accomplished but only after substantial redesign of the mission, it’s FSW, or sequences [13].

Table 2. Cassini's SPF Exemption List

SPF Exemption No.	Failure
1	Loss of a Radioisotope Thermoelectric Generator (RTG)
2	Loss of High Gain Antenna or either Low Gain Antenna inside 1.5 AU
3	Leakage or bursting of a propellant module tank (pressurant tank, main engine oxidizer tank, main engine fuel tank, thruster hydrazine tank)
4	External leakage or bursting of propulsion module fluid or pressurant lines and fittings of components in the lines, and of pressure transducers (leakage past a closed thruster, engine or fill valve is not exempted).
5	Structure (spacecraft adapter, orbiter, or probe truss)
6	Spacecraft separation band (retention/release)
7	Thermal blankets, surfaces, and shields (spacecraft and probe)
8	S/C cabling short
9	Selected command and data errors ¹
10	Main engine combustion chamber (catastrophic explosion)
11	Passive radio frequency equipment (3dB hybrid)
12	Micrometeoroid shielding (inherent or specific)
13	Power interruption greater than 37ms
14-18	Probe adapter structures, probe structure, spin-up and release mechanisms (exemption not applicable to premature release), heat shield, parachute systems

¹ Uplink Commands:

* Untimely destruction of flight software or sequence memory through incorrect addressing or misuse of uplink commands.

* Untimely commands leading to an inappropriate subsystem state.

3. AT LAUNCH: HIGH SSR BIT FLIP COUNTS

Immediately after Cassini's successful launch aboard the Titan-4B launcher in October 1997, the SOFS team was in the process of preparing for calibration of the engineering subsystems and the first trajectory course correction using the PMS ME system, with the first Venus-1 flyby planned for April 26, 1998. But as soon as the spacecraft left the launch pad, the telemetered engineering data reported a higher than expected number of single-bit-per-word errors on the SSR (referred to as Single Bit Errors, SBE), and a significantly higher number of double-bit-per-word errors (Double Bit Errors, DBE); both which were considerably over spec. The SSR spec indicated that relatively low SBE/DBE error rates were expected to occur: SBE=6/week and DBE=2/year. But at launch, these error rates were observed to be SBE=20/hr. and DBE=2/day. To make matters worse, a high sensitivity of the SSR SBEs was noted during the first month of the mission when a solar flare was observed by the GOES-9 satellite (reaching SBE=1201 in one hour), leading to a concern for the high dust and radiation environment that the spacecraft would encounter once it reached the Saturnian system.

The SSRs are a high capacity bulk storage medium containing 640 DRAMs of memory which are divided into 128 Sub-Modules (SM). Commercial SSR DRAMs are known to be highly sensitive to Single Event Upsets (SEU), so that Cassini's SSRs were fitted with extra shielding of approximately 0.500 inches of Aluminum around each SSR box in order to reduce the number of SBEs. Additionally, both SSRs were delivered with a HW Error Detection and Correction (EDAC) function which "scrubs" (fixes) the SSR memory every 537 seconds to correct all SBE occurrences. But any DBEs must be rectified by uplink commanding to fix the corrupted memory. These erroneous "bit flip" occurrences are undesirable since they cause corruption of the stored CDS/AACS/Instrument FSW loads (which are needed in case RAM memory encounters problems), and corrupts collected (stored) science data.

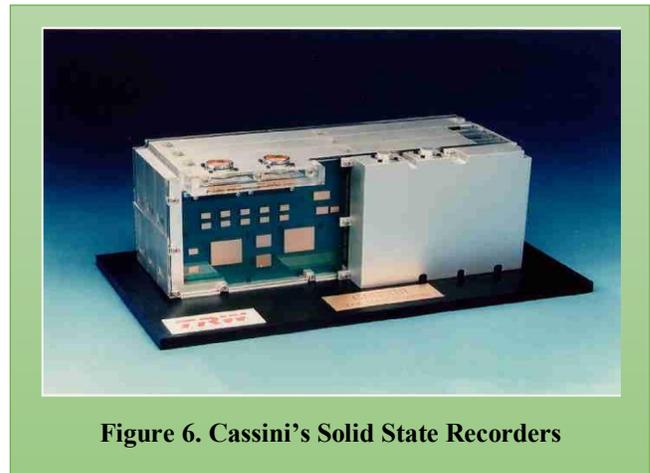


Figure 6. Cassini's Solid State Recorders

An anomaly investigation team was formed to determine the cause of these high error rates, concluding that the SSR's susceptibility to cosmic ray bombardment was increased by an anomaly within the SSR memory mapping due to human error. The physical adjacency of some data and checksum bits was laid out so that one cosmic ray hit could cause two bit errors (DBE) to occur (a violation of design requirements). The intent of the design was to separate the physical location of the two 20-bit SSR half-words in the DRAM memory device to prevent a SEU from causing a DBE. The as-built device physically located the two 20-bit SSR data words in adjacent memory locations, thus allowing a single SEU to upset multiple bits in a SSR 40-bit data word, resulting in a higher than expected DBE rate [14].

Ground Workarounds & FP Solutions: The original SSR repair strategy called for the SSR's EDAC circuitry to perform Single Error Correction & Double Error Detection (SECDED) in order to detect and correct SBEs automatically and to detect DBEs, flagging the DBEs for the SOFS team to take further appropriate actions. Correction of any DBE error requires prior knowledge of the contents of that SSR memory word. The majority of both SSRs contain stored science & engineering telemetry data, residing in SM8=> SM127. The CDS computer has no knowledge of the correct contents of

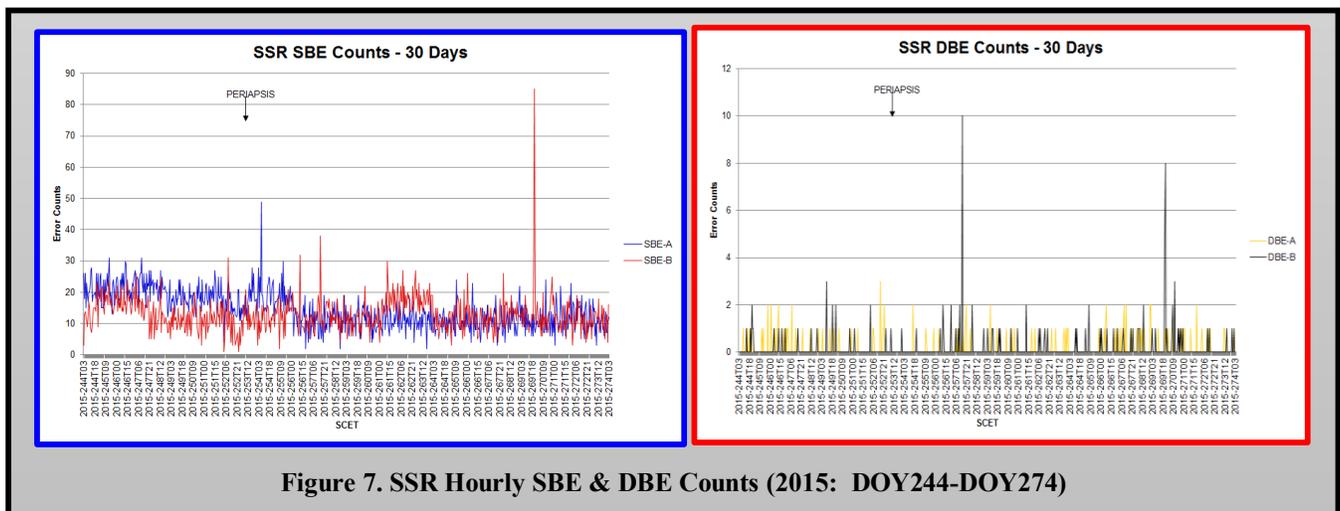


Figure 7. SSR Hourly SBE & DBE Counts (2015: DOY244-DOY274)

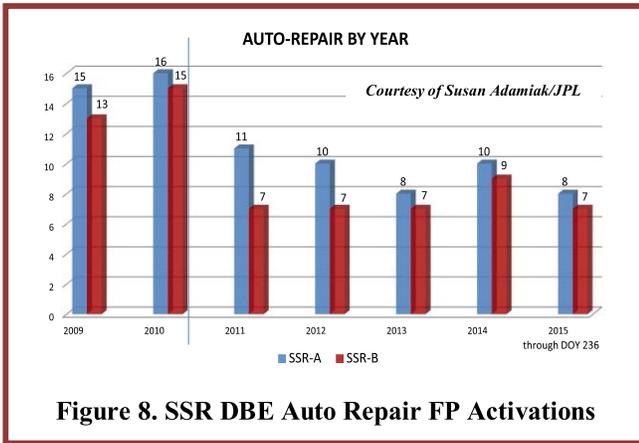


Figure 8. SSR DBE Auto Repair FP Activations

the science & engineering information, and therefore correction of DBEs in this region of the SSR is impossible. Only the eight SM0 => SM7 containing computer & instrument FSW loads can be restored back to their original contents. Therefore, the solution for fixing DBEs was two-fold for the SOFS team. Since DBEs occurring in SM8 =>SM127 are eventually “written over” by the data recorder within a 14 day time period, any DBEs occurring in this memory region would eventually be cleared in this manner. Fixing DBEs in the FSW Load SM0 => SM7 region first required identification of the affected SM, and then locating the DBE within that SM (via a bad checksum detected), followed by a “repair” of that SM’s memory region using the correct FSW Load word to overwrite the bad memory area (via uplinked commands). An uplink command was then sent to clear the DBE counter for that SM. If the DBE counter did not clear, then a bad bit was assumed to exist for that area of memory, requiring that region of the SSR to be permanently bypassed (FSW must be reloaded around the failed SSR memory region). Thus, the higher than expected DBE count required the SOFS team to become very diligent in monitoring both SSRs for DBE occurrences daily.

In order to observe dramatic fluctuations in bit error counts during events like solar flares (or any other adverse environmental influence), continuous SBE data collection was needed from the spacecraft’s telemetry stream. Since DSN passes were non-continuous, this goal was impossible to achieve. Although these data were recorded on the SSRs, playback of the SBE counts during subsequent downlink passes would have inhibited science playback, rendering this option infeasible. For the SOFS ground support community, it was apparent that the SBE/DBE error count reporting capabilities needed to be expanded, in addition to autonomously fixing DBE error occurrences in the FSW SMs. Therefore, a new set of requirements was developed to support future FSW upgrades to capture the full spectrum of SBE and DBE rate information on an hourly basis (Figure 7), followed by the implementation of new FP to detect and autonomously (periodically) resolve DBE occurrences within the SSR FSW memory. Once uploaded to the spacecraft, this new “SSR DBE Auto Repair” FP featured the ability to fix DBEs automatically without SOFS intervention, providing continuous monitoring of the SSRs. Since each SSR contains

4 copies of computer & Instrument FSW, any DBE could be restored back to its original content once detected by this onboard FP.

Flight experience: The SSR Auto Repair FP has performed very well in flight. Figure 8 shows the typical frequency of these repair activities (between 2009–2015) to be approximately SSR-A=10/yr. & SSR-B=7/yr. in the Solstice Tour (several DBEs are fixed in each repair activity). As was anticipated, high SBE counts occurred for areas of high dust and radiation. Figure 9 shows SSR-A & SSR-B’s SBE hourly count from the high dust environment of Pallene while Cassini flies by this moon, consistently reaching ~340-400 SBEs during each flyby event.

No ‘stuck’ DBEs had occurred on either SSR device until SSR-A’s SBE & DBE error counts suddenly reported a substantial rise on December 2, 2006 (Figure 10). Instruments and subsystems concurrently reported a large number of SSR data playback errors, data spikes, loss of data due to frame and packet header corruption, and erroneous time-tags which were time-stamped in the future. The corrupted frame header information also caused automated ground processing tools to fail. Several factors were considered when determining the possible cause of this phenomenon. Solar flare activity in combination with either adjacent data bit flips in playback data, or in the presence of the SSR memory mapping design error were suspected, leading the SOFS team to believe that the increased error rates might be a temporary condition (so that the SSR count might return to normal levels with decreased Solar activity). Yet the high SBE and DBE counts on SSR-A persisted after the solar activity returned to normal levels.

The SOFS team proceeded to collect hourly SBE totals from each of SSR-A’s SMs separately from spacecraft telemetry data (Table 3). These data indicated that SSR-A contained

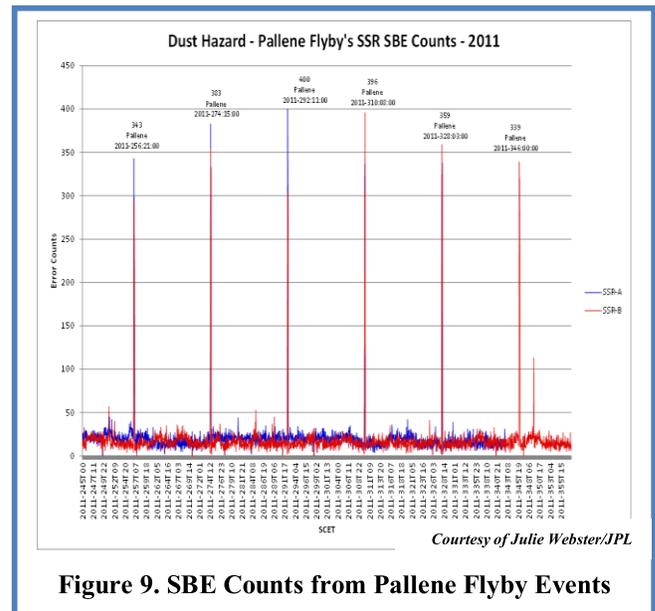


Figure 9. SBE Counts from Pallene Flyby Events

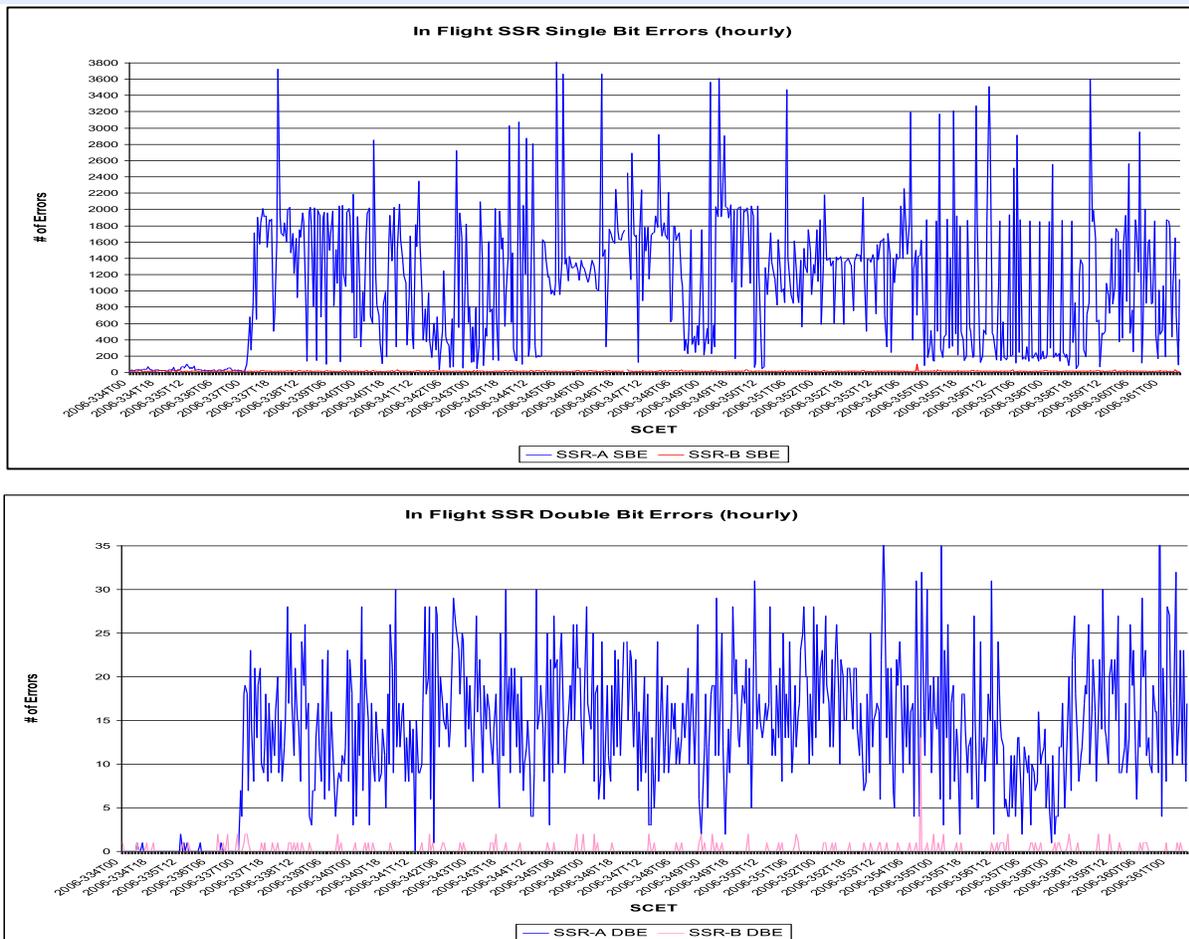


Figure 10. Total SSR-A/SSR-B Hourly SBE & DBE Counts for December 2006

(single) stuck bits in SM69 & SM80, but an extraordinary number of memory cell failures in SM39 (this SM represents <1% of SSR-A’s storage capability). Data from SSR-B indicated no stuck bits or bad memory cells. The SSR spec projected SSR SM failures rates at ~10% per SSR by April 2013 (13 per SSR). With this high SM failure projection (and to rectify the bad SSR-A SM39 memory problem), the SOFS

team decided that new FSW upgrades were needed to implement the capability of turning off any bad SM on either SSR (to remove it from use). Additionally, from that point forward, it was also decided that SSR-B would be used as the primary recording device to collect science data for all future observations, data recordings, and playbacks (with SSR-A as the backup unit), since it was known to contain no bad memory cells and was much less susceptible to radiation effects because of its placement on the spacecraft (relative to SSR-A). The new FSW changes were uploaded to the spacecraft in 2007, and activated through a new uplink command which allowed the SOFS team to remove a failed memory SM (or module); inhibiting it from being accessed for data storage or playback on the selected SSR. To date, only SSR-A SM39 has failed and removed from use.

Table 3. SSR-A Hourly SBE Counts for All SMs

12/22/06 SSR-A SBE Error Counts

Submodule	Hour 1	Hour 2	Hour 3	Hour 4	Hour 5	Hour 6	Hour 7	Hour 8
0	0	0	0	0	1	1	1	0
1	0	0	0	0	0	0	0	0
.....
38	0	0	0	0	0	0	0	0
39	2046	440	509	1461	1769	252	854	908
.....
68	0	0	0	0	0	0	1	0
69	2	9	15	22	29	36	44	8
70	0	0	0	0	0	0	0	0
.....
79	0	0	0	0	0	1	1	0
80	2	9	18	25	31	39	46	8
81	0	0	0	0	0	0	0	0
.....
127	0	0	0	1	2	2	2	1
Sum	2050	464	972	1509	1832	332	700	925

* Overflow bit is set

SSR Swap

←Very Large Number of Permanent Bit Errors

← Single Permanent Bit Error

← Single Permanent Bit Error

4. LAUNCH+3WKS: REGULATOR MALFUNCTION

Three weeks after Cassini’s launch, the SOFS team was in the process of preparing the PMS system for the first of many ME Trajectory Control Maneuvers (TCM) required to guide the spacecraft to its intended trajectory towards Saturn. Cassini’s PMS is the most complex system ever flown on an interplanetary probe, and the many regulated/non-regulated

ME TCMs would be needed to clean up dispersions from the upcoming planet flybys, to initiate the plane-change in the 90 minute Deep Space Maneuver (DSM), to perform the Saturn Orbit Insertion (SOI) burn and support Tour [15]. But before the PMS ME system could be utilized, it had to be “unisolated” first by opening the flow path from the helium tank to the propellant tanks. This was accomplished by firing PV-1 open (Figure 11). Next, the prime helium Latch Valve #10 (LV-10) must be commanded open so that the helium pressurant can flow through the lines, filling the fuel and oxidizer tank ullage space sufficiently (to target pressures). In this way, ME burns are initiated by allowing the propellants to be pushed through the lines to the ME combustion chamber where these hypergolic liquids mix together and ignite. Additionally, once helium flows through the lines, the prime regulator is expected to “lock-up” to the desired tank pressure levels (without exceeding the target pressures). From that point, it was the intention that LV-10 remain open for the entire mission with the healthy prime regulator in place to maintain the desired tank pressure levels.

FP was installed to protect against over-pressurization of the fuel & oxidizer tanks. Two Over Pressure (OP) FP algorithms were implemented into FSW in order to address fault conditions [16]. The OP-1 algorithm was the first line of defense in detecting any tank over-pressurization condition due to a leaking helium valve, so that its response commanded the prime LV-10 to close. The OP-2 FP response addressed problems with the prime regulator by pyro-isolating the tanks from the helium pressurant (by closing PV-2). In this case, the SOFS ground team must then command a swap to the backup regulator for use in the remainder of the mission. These two OP FP routines can be enabled or disabled (via uplinked command) and it is the SOFS team’s responsibility to handle these enable flags appropriately.

Cassini’s SOI insertion burn was to commence in 2004 upon reaching the Saturnian system (Figure 12). This was the most critical single maneuver in the entire Cassini/Huygens

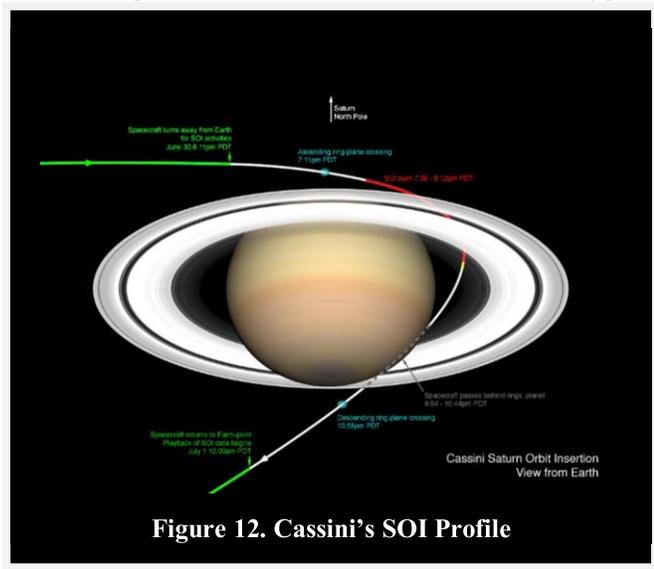


Figure 12. Cassini’s SOI Profile

mission since this insertion burn was required to reduce the spacecraft’s incoming energy sufficiently for it to be captured into Saturn’s orbit, thus placing Cassini into the desired orbital period. Since the RTL at Saturn is a little less than 3hrs, the SOFS team could not assist the spacecraft if an anomaly occurred during this crucial 97 minute deceleration burn. Instead, Cassini must autonomously detect, locate, and isolate any fault condition or failure that might occur, and then restore ME firing capabilities autonomously (if affected) via an uplinked series of commands (i.e. critical sequence). To provide Cassini with a robust PMS system, pre-launch designers took advantage of the opportunity to perform in-flight PMS system characterization studies. It was thought that by the time Cassini reached the Saturnian system after 6.7 years of flight, the prime regulator as well as LV-10 performance would be well characterized and understood, with backup units available should any problems arise. It was also surmised that performing a “SOI - 30 day Pressurization Characterization” exercise would guarantee the regulator’s health, fuel & oxidizer tank pressures, and good LV-10 operation. These planned characterization tasks led to high confidence in Cassini’s PMS design so that two waivers were issued for the regulator to close properly, deeming associated device faults to be low to negligible. Although a potentially mission catastrophic SPF, this item was added to the SPF exempt list pre-launch to certify that no tank Under-Pressure (UP) or OP FP was needed to support the SOI burn:

Waiver #1: Probability of any “Under-Pressure” condition is negligible.

Waiver #2: Probability of any “Over-Pressure” condition is extremely low.

Approximately three weeks after launch on November 8, 1997 when the SOFS team fired PV-1 and opened LV-10 to start the flow of helium to the ME tanks, the pressures rose to the expected levels but then continued to rise well above the projected target levels at which the prime regulator was expected to lock-up (at the astonishing rate of 7.6 psia/hr.), continuing to rise towards the OP-1 trigger point. The SOFS team issued a contingency uplink command to close LV-10 in order to halt the pressure rise. Subsequent analysis determined that the prime regulator was leaking at a rate which was well over the spec (1700 cc/min compared to the expected 1.70 cc/min “worst case leak rate” observed in testing). It was later speculated that a particle must have become lodged within the regulator due to the firing of PV-1 and its associated blowby products. Now a significant redesign was required for all regulated Main Engine (ME) burns for the entire mission, especially for crucial events like the 90 minute DSM maneuver and the 97 minute SOI burn. The “SOI 30-day Pressurization Characterization” task was now unviable since LV-10 must remain closed, as well as the existing FP strategy, so that a redesign of the SOI mission phase was now required. A quick redesign of the TCM-1 maneuver was performed (executed on November 9, 1997). TCM-1 was intended to be a regulated burn to adjust the spacecraft’s trajectory, cleaning up errors from Cassini’s

Prime HeLV (LV-10) Backup HeLV (LV-11)

CASSINI PMS SCHEMATIC
Cruise Configuration REVISED 09/28/00

High Pressure 2416 psia Ox (N₂O₄) Tank 229 psia Fuel (MMH) Line 275 psia Vented REA-B Line 0 psia
 LV10-REG 225 psia Ox (N₂O₄) Line 311 psia RTA Pressure 2380 psia Pad Pressure 50 psia
 REG-Chk Valve 241 psia Fuel (MMH) Tank 239 psia Hydrazine N₂H₄ 340 psia

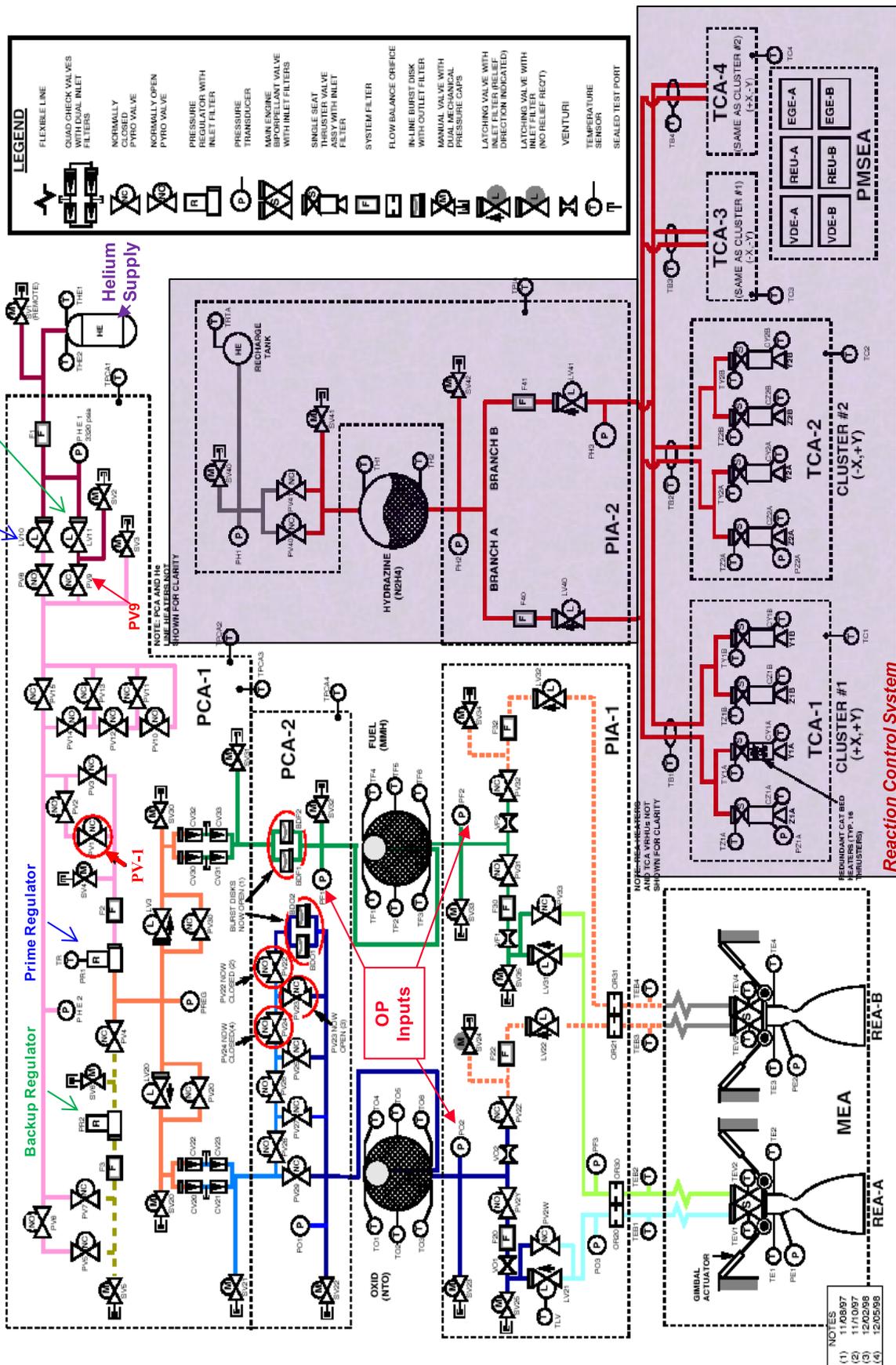


Figure 11. Cassini's Propulsion System Schematic

launch and the Centaur/Spacecraft separation dispersions. But since LV-10 could only be opened for a few minutes to pressurize the tanks, TCM-1 was executed by way of an uplinked sequence of commands which allowed LV-10 to be opened for only a few minutes. The Cassini Project now faced a new set of risks for any regulated ME burn maneuver requiring re-pressurization of the tanks. The option of swapping to the redundant backup regulator was considered, but determined to be vulnerable to the same risks as its counterpart, since the particulate-induced leak would quite likely have the same (or worse) effects once another pyro valve was fired to open and unisolated that regulator. An investigation was conducted to determine how this regulator malfunction could have slipped through Cassini's rigorous pre-launch failure analyses and test programs.

Cassini's regulator design was based upon Galileo's Teflon "soft-seat" configuration because of its superb performance in flight; exhibiting excellent leakage behavior. However, the cold-flow tests for Galileo's regulator indicated that this type of soft-seat design would likely experience a blocked flow passage due to seat extrusion, which is potentially a mission catastrophic failure. Unfortunately, Galileo's test data was unavailable at the time of Cassini's regulator design phase to investigate this problem further, facilitating a slight redesign for Cassini to replace the soft-seat with a "hard-seat" device, in order to avoid susceptibility to this failed-block condition. PMS designers considered adding UP FP to address the blocked regulator condition, but schedule and cost constraints deemed this option infeasible. Adding to the concern was the possibility of a plugged regulator sensing port (as was seen on the Mars Observer Spacecraft) which also drove decisions on Cassini's regulator design to incorporate the hard-seat configuration. A slight performance difference accompanied this change in regulator seat design. The new hard-seat had an associated increase in expected leak rate by a factor of "10" over that of the soft-seat design, due to its sensitivity to particulate contamination (1.0×10^{-3} scc/s vs. 1.0×10^{-2} scc/s). This increase in leak rate probability prompted the decision to install the backup regulator for additional system robustness, along with the two OP FP algorithms (described above) which would detect any over-pressure condition. Additionally, a second high-pressure helium latch valve (LV-11) was added to the PMS structure along with a pyro-isolation ladder installed upstream of the regulators (PV10-PV15). Several filters were also installed. However, the inlet filter usually installed by the manufacturer for the hard-seat regulator design was intentionally omitted for Cassini, due to concerns over the oxidizer's incompatibility with the microbrazed within this filter. With these new features added to the ME PMS system, the regulator design and leak protection were considered robust enough to allow the two waivers to be issued, exonerating the regulator of any failure to close properly.

With the occurrence of the SPF (exempted) regulator leak now in play, the Cassini Project faced a significant set of new risks for any ME burn maneuver that required re-pressurization of the tanks. "Very large leak rates" and

"stuck-open regulator" failures were now credible malfunctions for either regulator and the question of whether the upcoming maneuvers could be achieved using a leaking, and hopefully, stable prime regulator must be answered. Any associated pressure rise could potentially result in an OP-1 response trigger during future ME burn maneuvers. An effort was therefore undertaken to revisit the remaining mission activities to ensure that all maneuvers would be successful if the regulator performance degraded even further. The next major concern for the SOFS team was how to perform the upcoming 90 minute DSM maneuver and whether the regulator leak would worsen during that event.

The DSM burn was initiated on December 3, 1998 (launch +14 months). After that event, the prime regulator was determined to be leaking at an even higher rate; an increase of 6.6 times larger than before. It was speculated that an even larger particle had become trapped within the regulator. Fortunately, this problem occurred several years before the SOI burn was to commence, thereby allowing sufficient time to evaluate the problem and determine a fix to the mission design. It was decided that LV-10 must be opened just before any ME pressurization activity and then closed as soon as the desired tank pressure levels were reached, so that all ME burns had to be initiated via uplinked sequences to ensure that the proper timing was maintained. This was a good solution for relatively short ME burn maneuvers during cruise but not for the SOI Burn, which required tank pressures to be maintained at sufficient levels during a large portion of this long duration burn. The solution was to open LV-10 for 70 seconds just before SOI Burn initiation, allowing it to remain open long enough to accomplish the majority of the burn (hoping that the regulator leak would not worsen during this event). This new SOI burn strategy led to the identification of new failure modes which included the following:

- If the helium LV-10 is stuck closed, an automated swap to the redundant LV-11 helium latch valve is required via FP (UP FP), with PV-9 opened to unisolate that line.
- If the helium LV-10 is stuck wide-open, a mechanism is needed to stop the pressure rise
- If the Prime Regulator fails wide-open or completely closed, a swap to the redundant Backup Regulator must be accomplished via FP (OP FP)

To address the stuck-closed LV-10 condition, a new "High-Pressure Latch Valve (HPLV) FP algorithm was developed to facilitate a swap from LV-10=>LV-11. This FSW addition was possible since extra FP slots were incorporated into FSW (pre-launch) should the need arise for additional FP algorithms. This FP utilized the "alert message" architecture where a notification from AACS (upon detecting the stuck-closed LV-10 condition), could be delivered to CDS, activating the new FP response; a capability which was implemented within the uplinked critical SOI burn sequence. Likewise, if a stuck-open LV-10 or regulator condition

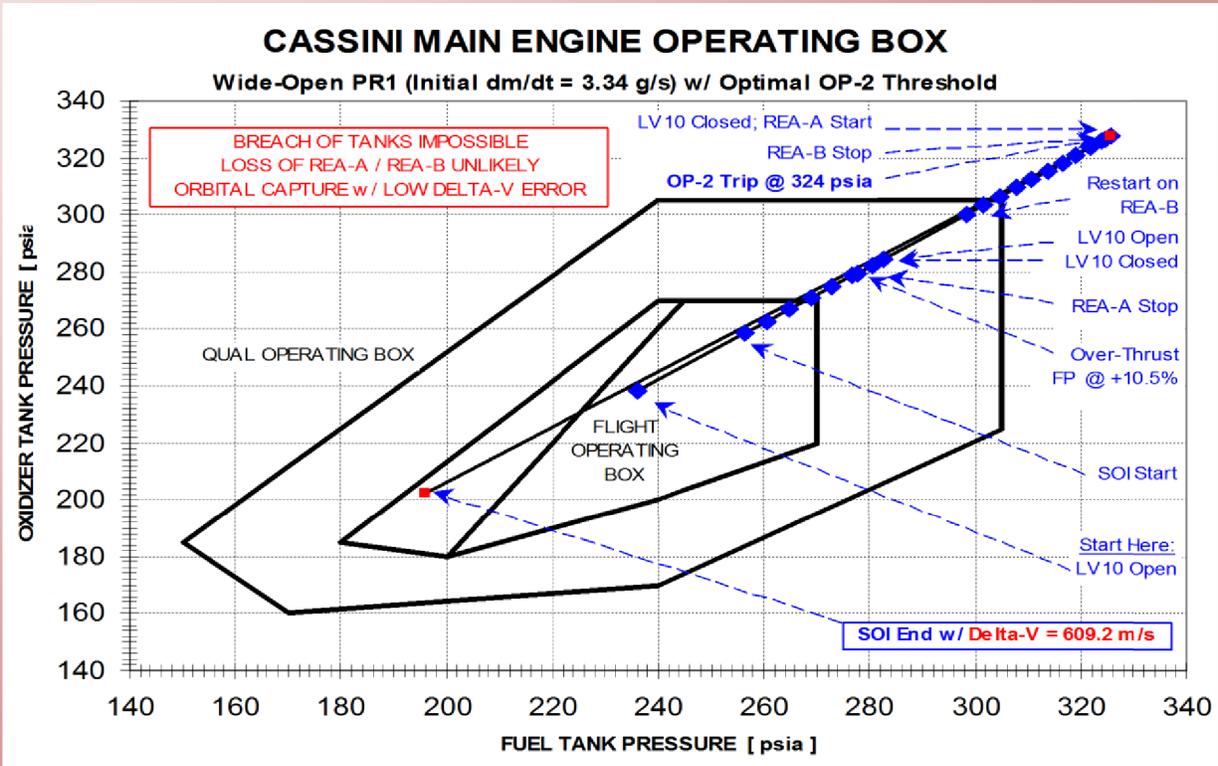


Figure 13. OP-2 “Bang Controller” Strategy during the SOI Burn Critical Sequence

occurred so that a significant pressure rise was in progress (threatening an imminent explosion of the propellant tanks) the pressure rise could be halted using the OP-2 algorithm, and then continue the SOI burn in “blow-down mode” (i.e. tank pressure levels are sufficient to perform the remainder of the burn). It was determined that halting the pressure rise at $P=324\text{psia}$ would leave the tank pressures at the desirable level, leaving the end of the burn close to the “chugging boundary,” allowing for successful completion of this critical maneuver for worst case conditions. This new “bang controller” FP concept was implemented by modifying OP-2’s monitor threshold level from 305psia to 324psia (Figure 13). The strategy was for OP-2 to trigger its response at the new threshold level, which in turn, executed the Safing Response (closes LV-10), and then to fire PV-2 in order to isolate the helium pressurant for the remainder of the burn.

Flight experience: Selected pre-SOI characterization studies of LV-10 performance showed good leakage behavior well within spec, and the regulator leak remained the same during cruise. In July 2004, the SOI burn was initiated via uplinked critical sequence using the OP-2 algorithm’s new trigger point as the mechanism to halt any dangerous tank pressure rise. The SOI insertion burn was very successful with no faults encountered during the event, and regulator performance indicated no increase in leak rate during or after the burn (or significant pressure rise towards the new OP-2 threshold trigger level).

5. LAUNCH+4 MONTHS: SPURIOUS SSPTS TRIPS

On February 14, 1998, the first of many spurious Solid State Power Switch (SSPS) load trip events occurred on Cassini due to the unforeseen environmental effects of galactic cosmic ray bombardment. Cassini’s power system consists of power control boards containing 192 SSPS switches. Ground radiation tests conducted in April 1998 confirmed that low energy particles could cause state changes of a power switch from On=>Tripped or Off=>Tripped. It was determined that one or more photon hits on the voltage comparator can result in a false indication that the current load is anomalously high, thus tripping off the switch. Predicts from the April 1998 radiation testing also supported in-flight results and suggested that an upset rate of up to one switch every 4 months could be expected. An SSPS load when suddenly tripped off can result in a condition which is benign to serious, depending on which switch is tripped, whether that particular load was in use at the time, and whether it activates FP. Although some of Cassini’s engineering devices have redundant units with redundant SSPS switches so that a tripped SSPS switch will not cause the load to go down, instruments and their associated replacement heaters (in almost every case) have only a single switch. Instrument damage can occur in only a few hours (~12 hr.) if replacement heaters are tripped (this situation is especially problematic for the Cruise mission phase where only 1 DSN pass per week is scheduled). Therefore, it was determined that protection of spacecraft’s subsystems and instruments from cosmic ray bombardment/SSPS trip events was warranted, requiring a

new “SSPS Trip FP” monitor & response algorithm. The monitor was configured to examine one SSPS switch state per second, (starting with switch number 1), proceeding through all 192 SSPS switches. The response contains a table of appropriate actions based upon the specific SSPS switch and its function:

Monitor: The monitor checks the SSPS state of each spacecraft switch once every 192 seconds, but only takes action for the switches that are found in the “TRIP” position. Three consecutive cycles through the monitor logic with the trip condition persisting are required to trigger the response.

Response: The response contains a table with unique actions for each of the 192 SSPS switches. The table can also be modified by the SOFS team via uplinked command if necessary. A tripped condition cannot be cleared until the SSPS is first turned off (and then left off or turned on again if that is the appropriate action). All trip events are logged in telemetry. For most SSPS switches, FSW does not attempt to recover the device attached to the switch, but simply to return the device to both a power and thermally safe configuration which is consistent with the actions of the spacecraft’s FP (Safing Response). The response will run up to two times for a re-detected trip condition (a modifiable parameter via uplink command), after which the response for that specific switch is disabled. This prevents multiple attempts to recover a switch from a true short condition. Once this FP has executed, the SOFS team must proceed with recovery actions and then re-enable that switch’s response.

Table 4. SSPS Trip Occurrences since Launch

Cassini SSPS Trip Events			
Event No.	DATE	SSPS Switch	No. of Trip Events for this Device
1	February 14, 1998	SPARE 3	1
2	September 15, 1998	SRU-A	1
3	September 28, 1998	SPARE 23	1
4	March 31, 1999	SSR-A LINE A	1
5	February 5, 2000	REA A/B SEC OX VALVE HTRS	1
6	February 11, 2000	RWA 1 LINE 1	1
7	January 4, 2001	VDECU-B	1
8	January 9, 2002	VDE A MEVD LINE 1	1
9	April 8, 2004	PMS 10PS BTA HTR	1
10	April 29, 2004	PSU PSU-A LC	1
11	June 2, 2004	RWA 1 LINE 2	1
12	November 11, 2004	Probe RFE Replacement Heater	1
13	February 26, 2005	PCA Panel Htr 1	1
14	November 3, 2005	RWA 4 LINE 1	1
15	March 2, 2006	HELVD A sw	1
16	April 30, 2006	RFS USO	1
17	June 21, 2006	SRU-B RHtr	1
18	August 19, 2006	TWTA B line B	1
19	October 3, 2006	SRU A Decon Heater	1
20	November 25, 2006	RWA 4 LINE 1	2
21	September 11, 2007	TWTA B line A	1
22	October 5, 2007	CIRS Decon Htr 2	1
23	December 9, 2007	SRU-B RHtr	2
24	March 20, 2008	TWTA B line A	2
25	March 27, 2008	CAPS Replacement Htr	1
26	November 29, 2008	MPD-B	1
27	November 22, 2009	VIMS	1
28	January 2, 2010	INMS RHtr	1
29	February 5, 2010	CDA Replacement Htr	1
30	March 22, 2010	MIMI LEMMS RHtr	1
31	July 12, 2010	FPP Backup Htr	1
32	July 20, 2010	CDS EU B	1
33	September 7, 2010	REA-A Prime Replacement Htr	1
34	March 31, 2012	HELVD B sw	1
35	December 14, 2012	CIRS 170K Decon 1 Heater	1
36	September 9, 2013	DST-A Line A Load Current	1

Legend: - Non-trivial SSPS Trip Events

Table 5. SSPS Trip FP Actions for Worst Cases

Non-Trivial SSPS Trip Events on Cassini							
Switch Number	SSPS Switch	Log Event	Cmd Switch "Off"	Cmd Switch "On"	Cmd Alt. Switch?	Alt. Switch SSPS No.	Switch State
7	TWTA-B Line A Load Current	Y	Y	Y	N	-	-
32	DST-A Line A Load Current	Y	Y	Y	N	-	-
35	EU-B Load Current	Y	Y	Y	N	-	-
68	USO Load Current	Y	Y	Y	N	-	-

Updated via uplink
command: N->Y

Flight experience: Table 4 depicts all 36 SSPS trip events that have occurred during Cassini’s mission to date. Several trip events were non-trivial and are indicated in yellow. The actions of the SSPS Trip FP for these particular switches are shown in Table 5 and detailed below:

- 1) May 2005 Ultra-Stable Oscillator (USO): Caused loss of ground-spacecraft communication with the SOFS team for a short period of time. The actions of the original response table required logging of the event only. After this event, the table was augmented to turn on the USO (via uplink command).
- 2) September 2007 Prime TWTA: A trip of the prime TWTA caused several FP routines to be activated, resulting in a Power-On-Reset of the RFS system and H/W swaps to the redundant TCU and TWTA devices. To avoid running FP for this SSPS line (as well as the prime DST Line A), FP routines were modified to allow the SSPS Trip FP to recover the device by simply turning it back on.
- 3) July 2010 Prime EU: Engineering Unit B (EU-B) supplies temperatures and pressures to engineering subsystems. Loss of data delivery to Thermal & PMS telemetry channels inhibits SOFS monitoring of associated device health status. EU-B FSW was reloaded by SOFS recovery actions to restore this capability.
- 4) September 2013 Prime DST: Although the prime DST unit tripped off, FP modifications (mentioned above for the prime TWTA) allowed the SSPS Trip FP to recover the device before FP could activate. The result of losing this particular load cause the Command Demodulation Unit to reduce the uplink rate to U/L=7.125 bps. Recovery actions required increasing this rate to 500 bps.

Table 6. CDA Repl Htr SSPS Trip FP Actions

Actions of the CDA Replacement Heater SSPS Trip FP							
Switch Number	SSPS Switch	Log Event	Cmd Switch "Off"	Cmd Switch "On"	Cmd Alt. Switch?	Alt. Switch SSPS No.	Switch State
189	CDA Replacement Heater	Y	Y	Y	Y	186	OFF
186	CDA Electronics Load Current						

Certain SSPS lines if tripped, will cause reconfigurations of selected spacecraft's loads. An example of this case occurred on February 5, 2010 when the Cosmic Dust Analyzer's (CDA) Replacement Heater SSPS line tripped. For this case, the SSPS Trip FP logged the event and commanded the associated Switch #186=>ON, following the Safing Response strategy (turning the CDA Replacement Heater ON and commanding the CDA instrument OFF; see Table 6).

6. SATURN—4 YEARS: PROBE RELAY ERROR

The Titan moon is of keen interest to scientists since it contains a murky atmosphere which may have been similar to that which existed on the Earth before life formed on our planet. Its surface is obscured by a photochemical haze, and until Cassini reached the Saturnian system, the surface features of this moon were believed to contain liquid lakes and seas (confirmed to be true in the Solstice Tour). Once deployed to this moon in January 2005, ESA's Huygens Probe was tasked to measure data from Titan's atmosphere, determine its wind effects, and investigate the surface features. Return of the probe science data was considered to be a key element to the success of the joint Cassini-Huygens mission.

Ground-based activities to prepare for the Probe deploy & relay task consisted of flight operations exercises, performing "what-if" tests, and validating the Probe's FSW. The Probe was actually comprised of two redundant probe-like units; each one performing its own separate mission in parallel (but independent of one another), referred to as "Chain A" and "Chain B". Since these Probe computers had minimal onboard data storage capability, it was planned that the data captured from both chains would be transmitted to the Cassini orbiter directly during Titan entry so that the spacecraft would provide the bulk of the data storage needed to support the Probe Relay task (relaying it back to Earth) throughout

the descent and landing stages of the Probe Mission. End-to-end in-flight tests of the Probe Relay link were performed in February 2000. These exercises were necessary in order to characterize the behavior of the combined Cassini-Huygens data transmission system. The Probe signal was delivered to the Cassini spacecraft in-flight, and then delivered to the DSN station (the signal and data detection thresholds of the Probe receiver were of specific interest here). Results from this "Cassini-Probe=>DSN Station" relay test indicated insufficient margin to maintain the carrier and subcarrier lock for the duration of the upcoming Probe Mission (Figure 14). The digital circuitry which decodes the data from the subcarrier did not have sufficient bandwidth to properly process the data from the subcarrier once it was Doppler shifted by the 5.6 km/s (nominal) velocity difference between Cassini and the Probe. The effect of this anomaly was that it would lead to an unacceptable loss of data during the Probe Descent => Titan Landing phase since the digital circuit design did not adequately account for the Probe data's full Doppler shift [17]. A Huygens Recovery Task Force (HRTF) team was established (a joint effort between ESA/NASA) to troubleshoot the problem in January 2001, leading to a three-part solution which allowed full recovery of the Titan data:

Part 1: A redesign of the mission profile was needed to provide the Huygens Probe with a trajectory conducive to a low Doppler shift in the Probe-Cassini spacecraft radio link. To achieve this goal, the early part of the Saturn Tour phase resulted in a higher Cassini orbiter flyby altitude of Titan (at 60,000 km), requiring a redesign of the first two orbital revolutions around Saturn into three revolutions. From that point, the original planned tour configuration could then be maintained (at a moderate ΔV cost).

Part 2: The Probe's transmitters must be pre-heated before its descent into Titan's atmosphere in order to optimize the transmit frequency.

Part 3: The Probe Support Avionics (PSA) receivers were designed to revert to a Doppler-shift mode in the absence of a carrier lock. Since the new mission design had a much lower Doppler shift than that of the original, the PSAs could no longer detect the carrier. Therefore, the Probe must be commanded to the Base Frequency (referred to as "BITE Mode" – a "Zero Doppler" test mode that holds the lockup frequency at a level equivalent to -1m/s relative velocity) by the Cassini orbiter, instead of utilizing the signal at the expected Doppler frequency. This mode of operation MUST be maintained in order to collect all the Probe Relay data, even during (and after) FP activations. To accomplish this task, an empty slot within the ATC FP FSW was utilized to send the "Probe BITE Mode" command continuously. ATC FP has the capability to control temperature conditions for up to 12 separate devices on the spacecraft in order to autonomously maintain these components within temperature tolerances. This is accomplished by commanding the associated heaters states to an ON or OFF condition once per every 12 seconds (only one command can be sent per second; a constraint on FSW; see Figure 15). Pre-launch, only 8 devices were identified for ATC protection,

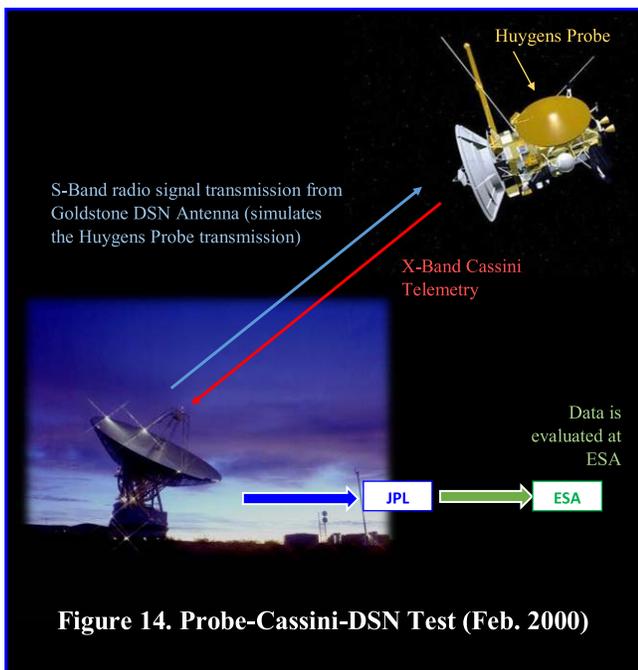


Figure 14. Probe-Cassini-DSN Test (Feb. 2000)

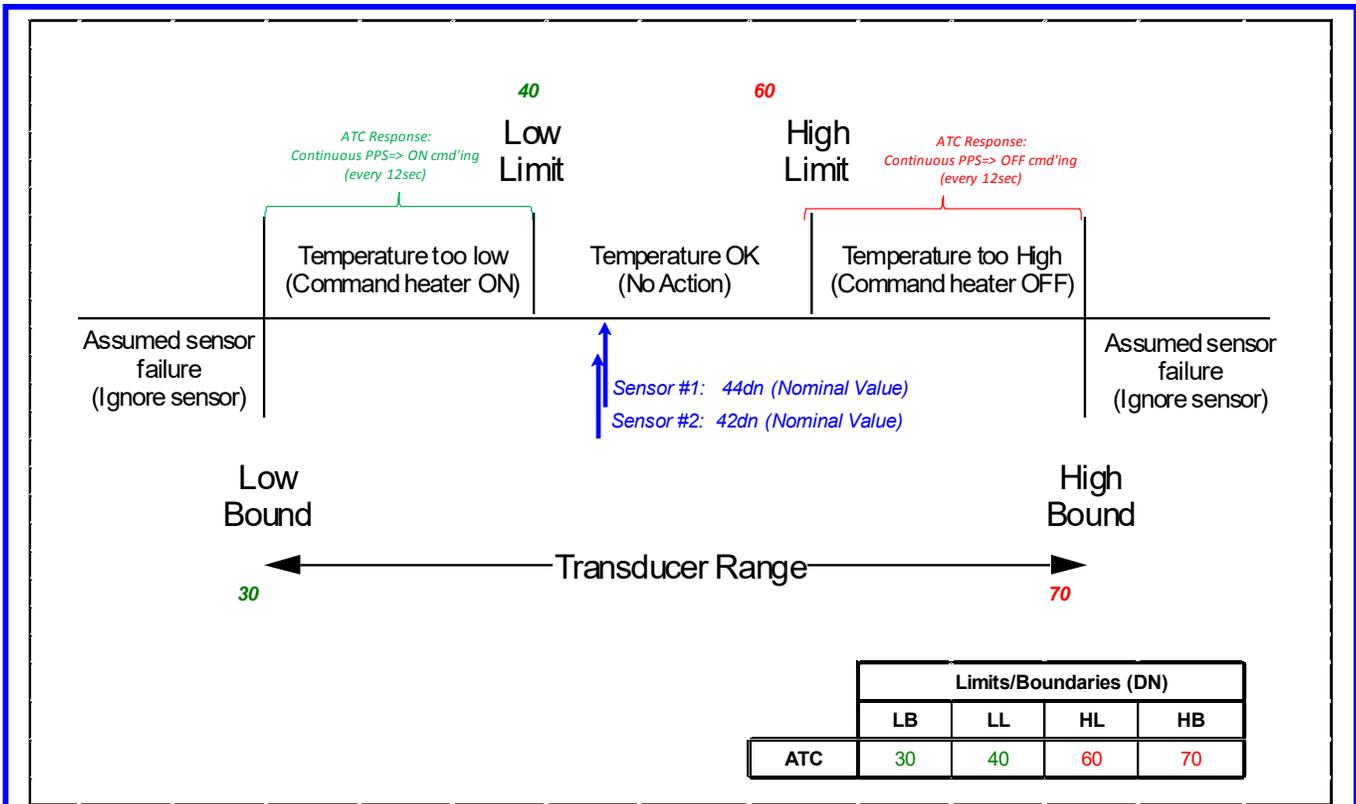


Figure 15. ATC Activity Example (When Enabled)

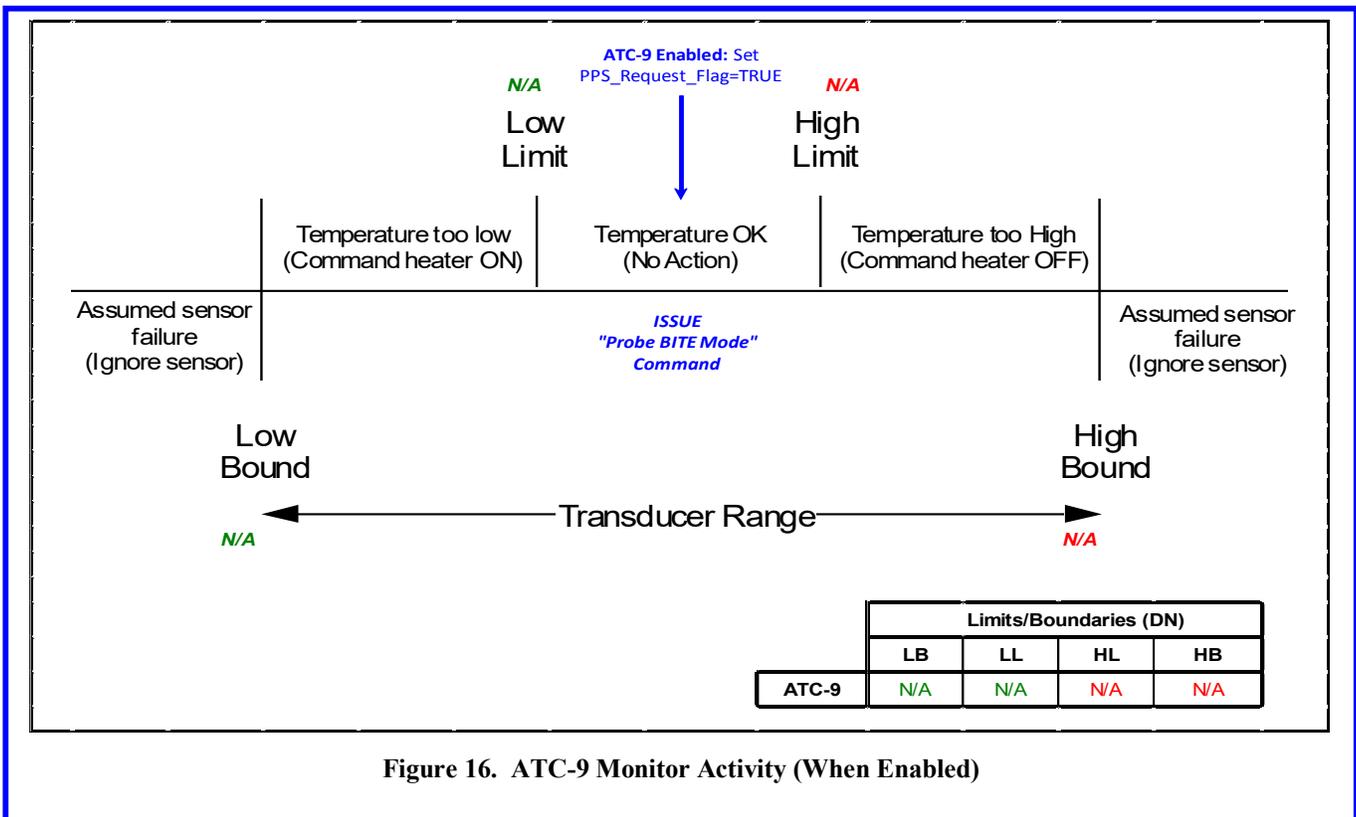


Figure 16. ATC-9 Monitor Activity (When Enabled)

with 4 “placeholders” remaining for any other devices requiring thermal protection. All ATC algorithms are configured with two sets of specified temperatures limits and boundaries. If limits are exceeded, a heater OFF or ON command will be issued every 12 seconds. If the boundaries are reached or exceeded, the ATC’s monitor logic will assume that the temperature condition can no longer be controlled and will continuously increment a fault counter to alert the SOFS team that the algorithm has ceased functioning. All 12 ATC algorithms can be enabled or disabled.

Using placeholder “ATC #9” was a perfect solution for satisfying the requirement of continuously sending the “BITE Mode” command to the Huygens Probe. Since all ATC algorithms issue their command requests even when FP is activated (and also post-fault), this “Probe BITE Mode” command could be issued continuously simply upon enabling the ATC-9 monitor. FSW modifications were made to ignore the limits and boundaries of the algorithm so that setting the enable flag caused the "Request for PPS Command" to be set to TRUE, thereby requesting the Probe BITE Mode command every 12 seconds (Figure 16). This new FSW was uplinked in 2003 for use in the upcoming Probe Relay Sequence.

Flight experience: The Huygens Probe Mission was very successful, with the exception that no data was received from Chain A since the Huygens Receiver USO was unintentionally not powered on (an oversight; human error). However, continuous data was received on Chain B throughout the descent, and for 50 minutes on Titan’s surface. After landing, minor data losses were experienced by the Probe during the following 20 minutes as Cassini finally passed beyond the Probe’s horizon (as expected). Since both data chains are redundant and completely independent of each other, most of the data was captured with the exception of the Doppler Wind Experiment which relied upon receipt of data from both computer chains [18].

7. SATURN–3 YEARS: POOR S/C=> EARTH LINK

Cassini’s RFS telecommunications system is comprised of a body-fixed HGA antenna, and two low gain LGA1, & LGA2 antennas. LGA1 is mounted on top of the HGA with an unobstructed field of view of 112 deg., and LGA2 is mounted on a boom at the aft end of the spacecraft and is not used for the Tour segments of the mission. Three earth-based DSN stations located at Goldstone (California), Canberra (Australia), and Madrid (Spain) support Cassini operations using 34-meter and 70-meter dish antennas. Since the HGA antenna has a directed gain over 6000 times stronger than the LGA antennas, it is used during all nominal spacecraft operations, communicating at tens or hundreds of kilobits per second (depending on the DSN station). The LGA1 antenna is utilized when faults occur (configured by FP) since certain anomalous conditions are severe enough to warrant staying on low uplink (U/L) & downlink (D/L) rates.

When FP activates, the SOFS team typically follows a multi-step “fault recovery procedure” to help verify the spacecraft’s

health and post-fault states before recovery actions are determined in order to resolve the fault condition and reactivate the onboard sequence. The Spacecraft Safing Response is called by most FP routines. This response terminates the onboard sequence, configures spacecraft power loads and functions to a safe, predictable state. Non-essential loads are powered off, with various subsystems placed into modes that are appropriate for the current mission phase, and required heaters are turned on in order to maintain the thermal health of the spacecraft’s instruments and systems. This response also commands the low D/L=5bps (bits per second) & U/L=7.8125bps rates using the LGA1 antenna; a configuration whose spacecraft=>earth link margins were adequate for the early phase of Cassini’s mission through cruise. Pre-launch requirements by mission designers allowed 2 weeks for fault recovery by the SOFS team, but this allocation was deemed unacceptable for the Tour phases of the mission. Once Cassini reached the Saturnian system and began its mission Tour phase in 2004, the three Orbital Trim Maneuvers (OTM) required for each loop around Saturn-Titan made this 2-week-turnaround period infeasible, since a lengthy spacecraft recovery period would likely cause Cassini to fall off its Tour trajectory. Quick fault diagnosis and recovery were essential to maintain not only the Tour configuration but also to protect the mission’s science objectives. It was determined that the spacecraft-earth link margins at Saturn would be unacceptable to support expedient fault recovery, so that a resolution to this problem was needed before reaching the Saturnian system.

Detecting and acquiring the spacecraft’s telemetry stream on the post-fault LGA1 antenna at the low downlink rate of 5 bps was clearly infeasible for Tour operations. This configuration yields a very weak and variable carrier signal using the Auxiliary Oscillator at such large Earth-Saturn distances. With this configuration, 18 hours are required to receive a full deck of telemetry data once the DSN has locked up on Cassini’s signal (~35 minute/frame; 30 frames of telemetry required). Although the spacecraft can be commanded to higher rates and configure to use the HGA antenna (all 30 telemetry frames would then be delivered in ~10 minutes), this strategy is undesirable for certain AACS related faults which must remain on LGA1 with the lower D/L & U/L rates. Therefore, a new FP algorithm was developed which allows the spacecraft’s FP Manager logic to determine if the HGA/high rate reconfiguration is acceptable, based upon internal statistics within the spacecraft which indicate the severity of the fault condition. A “High Gain Antenna Swap (HAS)” algorithm was designed and implemented into the FSW in 2003 to achieve this goal, helping the SOFS team improve post-fault recovery time substantially for most fault cases.

The HAS monitor watches for activations of the Safing Response (Figure 17). Once a FP algorithm has been activated (requesting the Safing Response), the “FP Active” flag will be set until the response chain has been completed. A “Safing Response Counter” is incremented at the

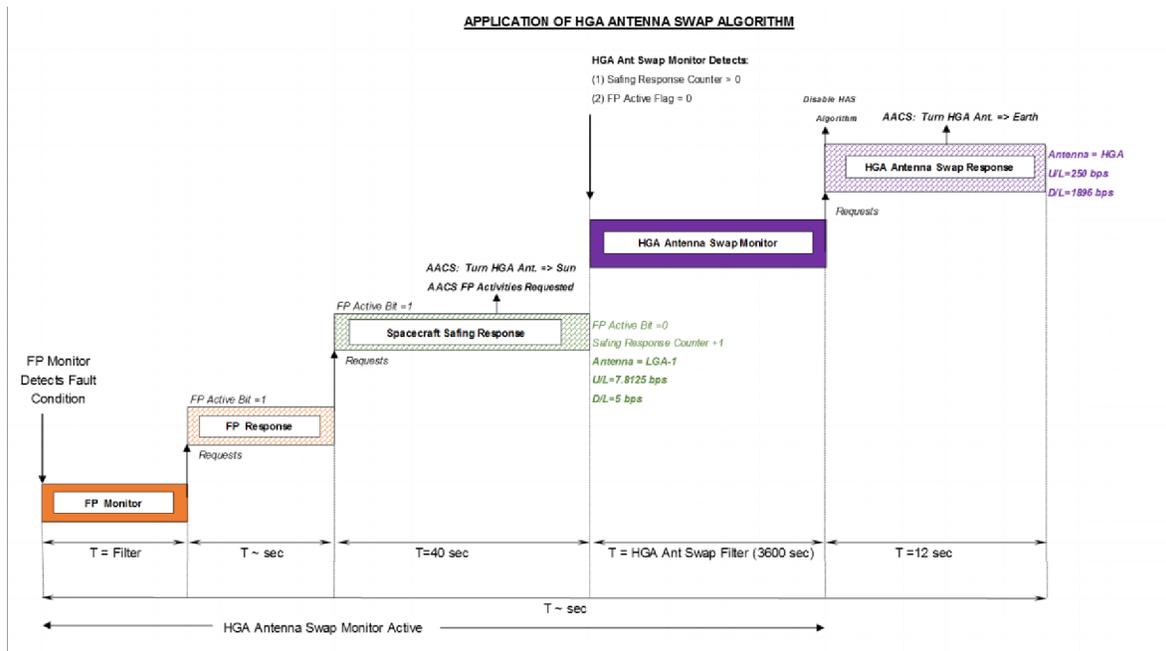


Figure 17. FP Algorithm Chain using High Gain Antenna Swap Algorithm

conclusion of the Safing Response, causing the HAS monitor to start incrementing its countdown timer (3600 seconds). If safe AACS criteria have been met (no severe AACS-related fault), the HAS monitor will request the HAS Response and then disable itself. Safe AACS conditions required that the AACS flight control system is able to achieve an “RCS Internal Mode” configuration and that AACS FP activities have been completed. The HAS Response is configured to execute one hour after any Safing Response activation to increase the downlink rate from 5bps => 1896bps, and the uplink rate from 7.8125bps => 250bps.

Flight experience: To date, Cassini has experienced 6 Safing Response activations (Table 7). HAS FP was implemented in 2003 and was executed successfully during the last two Safing Response activations in 2007 & 2010, greatly reducing post-fault recovery time.

8. IMPLICATIONS FOR CASSINI’S EOM

Cassini’s mission has progressed very well during its 18 years of flight, now heading towards its final F-Ring & D-Ring Proximal (FRPO) orbit phase, before taking its fiery plunge into Saturn. Although spacecraft aging typically leads to

Table 7. Cassini’s Spacecraft Safing Response Activation History

Safing No.	Date	Mission Segment	Fault Cause	SOFS Team Diagnosis	FP Activated
1	3/24/1998	Planet Flyby Phase	The redundant Stellar Reference Unit (SRU) was found to be misaligned when its counterpart SRU was turned on	This condition cannot be modeled in the Cassini test facility	Safing Response
2	1/11/1999	Planet Flyby Phase	FSW contained an overly sensitive AACS control target parameter	Only flight experience can reveal this problem	Safing Response
3	5/10/2001	Cruise	Missing a telemetry mode in the onboard sequence in redundant CDS backup	Operator error	CDS Internal FP + Safing Response
4	5/12/2003	Cruise	An attitude control pointing vector omitted in the onboard running sequence	Operator error	Safing Response
5	9/11/2007	Prime Tour	SSPS Trip of the prime TWTA unit due to a cosmic ray hit	Environmental effects	TWTA FP (TCU & TWTA swaps), RFS POR FP, + Safing Response + HAS Response
6	11/2/2010	Solstice Tour	An uplinked command experienced a cosmic ray hit (causing the prime CDS to swap to its redundant unit)	Environmental effects	CDS Internal FP + Safing Response + HAS Response

electrical and mechanical parts degradation, Cassini has had an excellent track record. Problems such as high friction in the Reaction Wheel Assemblies when used in the low rpm region have arisen and to date, and only the CAPS instrument has failed. In 2012, this device tripped off due to unexpected voltage shifts which rendered the instrument unusable, but overall Cassini’s past performance has been excellent with only minor problems and overall healthy subsystems and instruments. Cassini’s prime regulator leak hasn’t worsened during the mission in spite of several ME burns, and OP FP monitor thresholds have been lowered to support the lower tank volumes as the propellant is depleted. The spacecraft’s fuel and oxidizer residuals are running near empty now, so that the SFOS team keeps track of propellant usage very closely (using analytical projections and in-flight test information) until the last ME burn has been executed.

The upcoming FPRO mission segment is an entirely new challenge for Cassini with its unique set of very fast, ballistic orbital tracks; that which promises to yield exceptional science opportunities never before explored. The diverse environmental factors of this flight region have the potential to challenge the SOFS team even further, since the D-Ring environment (the closest ring to Saturn), is expected to be much dustier than previous moon/ring flybys & crossings, with possible higher radiation. Both of these environmental factors are expected to exacerbate the frequency of SSPS Trip occurrences, SSR bit flips, and possible SSR SM memory failures.

Numerous DBE occurrences have the potential to trigger near-continuous SSR DBE Auto Repair FP activations if they should occur in the SSR FSW region. This is a condition which will cause science data collection to be halted during SSR repair activities, as well as inhibiting instrument FSW loading from the on-board running sequence (missed science activities). It is the responsibility of the SOFS team to recover from these faults in the presence of planned maneuvers & science activities which could potentially be lost until the spacecraft is returned back to nominal operations once again. Therefore, SSR DBE Auto Repair FP will be temporarily disabled during the loading of instrument FSW and high value science recording, and several recovery procedures are currently in development to address single and multi SSR SM

failures (on-the-shelf procedures with recovery actions and pre-tested commands built and ready for uplink), as well as resolution actions for all 192 SSPS lines if tripped.

9. CONCLUSIONS & LESSONS LEARNED

For any spacecraft to complete its mission successfully without significant risk or degradation to its subsystems, instruments, and mission objectives, the vehicle must contain a robust FP strategy. In general, FP diagnostic capabilities are required to cover a large volume of fault possibilities due to the ever-increasing complexity of spacecraft designs. Pre-launch analyses and test efforts to preclude fault conditions do not always capture all fault cases, so that several unknown problems can surface after launch. During the long span of Cassini’s mission, several new FP routines have resolved problems not anticipated by pre-launch designers. Significant complications from unknown environmental conditions, human errors, and design oversites have been resolved through FP solutions. For Cassini, these upgrades were possible since enough time was available during cruise (and flexibility built into the FP FSW design) to address these issues. One of Cassini’s best examples of a major mission impact due to human error was the regulator malfunction; a robust regulator design which was based upon successful Galileo flight experience without the supporting test data to confirm design assumptions, leading to not only an invalidated FP design strategy, but also the issuance of two SPF waivers, impacting the entire mission profile and the spacecraft’s most critical SOI maneuver. Yet, arduous work-arounds for unforeseen problems like high SSR DBE counts, spurious SSPS load Trips, and critically slow post-fault recovery at great spacecraft-Saturn distances can be avoided through FP solutions, in order to preserve missions like Cassini-Huygens and its 3 tour phases.

ACKNOWLEDGEMENTS

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

REFERENCES

- [1] NASA, “Cassini Launch Press Kit,” October 1997.
- [2] P.S. Morgan, “Cassini Mission-to-Saturn Spacecraft Overview & CDS Preparations for End-of-Mission Proximal Orbits,” Jet Propulsion Laboratory/California Institute of Technology, IEEE Conference Paper, Big Sky, Montana, March 2015.
- [3] P.S. Morgan, “Fault Protection Techniques in JPL Spacecraft,” First International Forum on Integrated System Health Engineering and Management in Aerospace (ISHEM), Napa, California; ISHEM Paper, Presentation, dated November 2005.
- [4] K. Smith, C. Peng, “Modal Test of the Cassini Spacecraft,” Jet Propulsion Laboratory/California Institute of Technology, SDRC Operations, October 1996.

Table 8. SBE/DBE Counts during Mission Events

SSR Errors during Flight (per hr.)		
Mission Phase/Event	SBEs	DBEs
Nominal Flight	30-50	~2-4
Pallene Moon (Ring) Flybys	340-400	~2-6
Saturn G-Ring Flybys	1800-2500	~6-9
Broken Submodule	5000	~45

- [5] T. Scharton, K. Chang, “*Force Limited Vibration Testing of the Cassini Spacecraft and Instruments*,” Jet Propulsion Laboratory/California Institute of Technology, 17th Aerospace Testing Seminar, Institute of Environmental Sciences, Manhattan Beach, California, October 14-16, 1997.
- [6] M. Coleman, C. Peng, K. Smith, “*Test Verification of the Cassini Spacecraft Dynamic Model*,” Jet Propulsion Laboratory/California Institute of Technology, SDRC Operations, IEEE, 1997.
- [7] H. Himelblau, W. Hughes, A. McNelis, D. Kern, T. Bergen, “*Derivation of Acoustic Criteria for the Cassini Spacecraft and Comparison with Flight Data*,” Rocketdyne, NASA John H. Glenn Research Center, Jet Propulsion Laboratory/California Institute of Technology, date unknown.
- [8] V. Mireles, G. Tsuyuki, “*A Summary of the Cassini System-Level Thermal Balance Test: Engineering Subsystems*,” Jet Propulsion Laboratory/California Institute of Technology, #97ES-278, 1997.
- [9] G. Tsuyuki, V. Mireles, E. Lin, A. Avila, “*A Summary of the Cassini System-Level Thermal Balance Test: Science Instruments*,” Jet Propulsion Laboratory/California Institute of Technology, #97ES-33, 1997.
- [10] M. Adams, G. Spitale, H. Garrett, “*Meteoroid Protection Provided by Cassini Thermal Blankets: Testing and Modeling*,” Jet Propulsion Laboratory/California Institute of Technology, date unknown.
- [11] P.S. Morgan, “*Robotic Spacecraft Health Management*,” Textbook: ‘System Health Management: with Aerospace Applications’; Chapter 34, Wiley Publisher, May 2011.
- [12] NASA, “*NASA Technical Handbook Fault Manager Handbook*,” NASA-HDBK-1002, April 2, 2012.
- [13] C.P. Jones, “*Cassini Project Pre-ship Review/Single Point Failures*,” April 1, 1997.
- [14] G.M. Swift, S.M. Guertin, “*In-Flight Observations of Multiple-Bit Upset in DRAMs*,” Jet Propulsion Laboratory/California Institute of Technology, year unknown.
- [15] T.J. Barber, R.T. Cowley, “*Initial Cassini Propulsion System in-Flight Characterization*,” AIAA 2002-4152, 2002.
- [16] P.S. Morgan, “*Cassini Spacecraft’s In-Flight Fault Protection Redesign for Unexpected Regulator Malfunction*,” Jet Propulsion Laboratory/California Institute of Technology, IEEE Conference Paper, Big Sky, Montana, March 2010.
- [17] C. Sollazzo, “*The Huygens Probe Mission to Titan: Engineering the Operational Success*,” briefing for Spaceops Conference in Rome, Italy, 2006.
- [18] D. Allestad, S. Standley, “*Cassini Orbiter Operations Lessons Learned for the Huygens Probe Mission*,” 2006.

BIOGRAPHY



Paula S. Morgan is an Aerospace Engineer currently working for Cal Tech/Jet Propulsion Laboratory as the Lead Engineer of the Command & Data Subsystem and System Fault Protection Subsystem Teams for the Cassini Spacecraft Operations Element, and is the Technical Group Leader for Operations for the Section 349 Flight Electronics & Software Systems Division. Previously, she was the Group Supervisor of the Multi-Missions Operations Team, and has worked on NASA’s Constellation Mission-to-the-Moon Orion/Ares Program, was Lead Engineer for Fault Protection on the EPOXI Spacecraft (Deep Impact Extended Mission), was a member of the Mars Reconnaissance Orbiter Anomaly Investigation Team, a member of the Kepler Telescope Fault Analysis & Probability Risk Assessment teams, and has supported the CloudSat, and Stardust spacecraft programs. She has also worked for the Kenetech Windpower Company designing KVS 33-meter & 45-meter blade wind power plants. She also worked for Rockwell International’s Space Systems Division as the Team Leader of the Liftoff Clearance, Solid Rocket Booster, and External Tank Separation elements on the Space Shuttle Program, and was the Lead Engineer of the External Tank Separation Team. Paula is a member of the Phi Kappa Phi Honor Society

