Fault Protection Design and Testing For the Cassini Spacecraft in a "Mixed" Thruster Configuration

David Bates[1], Allan Lee[2], Peter Meakin[3], and Raquel Weitl[4]
Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California

NASA's Cassini Spacecraft, launched on October 15th, 1997 and arrived at Saturn on June 30th, 2004, is the largest and most ambitious interplanetary spacecraft in history. In order to meet the challenging attitude control and navigation requirements of the orbit profile at Saturn, Cassini is equipped with a monopropellant thruster based Reaction Control System (RCS), a bipropellant Main Engine Assembly (MEA) and a Reaction Wheel Assembly (RWA). In 2008, after 11 years of reliable service, several RCS thrusters began to show signs of end of life degradation, which led the operations team to successfully perform the swap from the A-branch to the B-branch RCS system. If similar degradation begins to occur on any of the B-branch thrusters, Cassini might have to assume a "mixed" thruster configuration, where a subset of both A and B branch thrusters will be designated as prime. The Cassini Fault Protection FSW was recently updated to handle this scenario. The design, implementation, and testing of this update is described in this paper.

Nomenclature

AACS	=	Attitude and Articulation Control Subsystem
AFC	=	Attitude Control Flight Computer
CBH	=	Catbed Heater
DOY	=	Day of Year
ETC	=	Excessive Thruster Commanding
FP	=	Fault Protection
FSDS	=	Flight Software Development Suite
FSW	=	Flight Software
GSW	=	Ground Software
ITL	=	Integrated Test Laboratory
LV	=	Latch Valve
MEA	=	Main Engine Assembly
MPD	=	Mono-propellant Driver Unit
MTA	=	Mono-propellant Tank Assembly
OTM	=	Orbit Trim Maneuver
RCS	=	Reaction Control System
RWA	=	Reaction Wheel Assembly
S/C	=	Spacecraft
VDECU	=	Valve Driver Electronics Controller Unit

I. Introduction

The Cassini spacecraft was launched on 15 October 1997 by a Titan 4B launch vehicle. After an interplanetary cruise of almost seven years, it arrived at Saturn on June 30, 2004. To save propellant, Cassini made several gravity-assist flybys: two at Venus and one each at Earth and Jupiter.

[1] Cassini AACS FP Engineer and Uplink Lead, 4800 Oak Grove Dr, Pasadena, CA, david.m.bates@jpl.nasa.gov

[2] Section Staff, Guidance and Control Section, Division of Autonomous Systems. Project Element Manager, Cassini Attitude and Articulation Control Mission Operations Team, 1999–2009. 4800 Oak Grove Dr, Pasadena, CA, allan.y.lee@jpl.nasa.gov

[3] Soil Moisture Active Passive Fault Protection Lead, 4800 Oak Grove Dr, Pasadena, CA, peter.c.meakin@jpl.nasa.gov

[4] Cassini Fault Protection Engineer, 4800 Oak Grove Dr, Pasadena, CA, raquel.m.weitl@jpl.nasa.gov

In order to meet the attitude control and navigation requirements of the orbit profile at Saturn, Cassini is equipped with a bipropellant Main Engine Assembly (MEA), a monopropellant thruster-based Reaction Control System (RCS), and a Reaction Wheel Assembly (RWA). The Main Engine is generally used for large maneuvers requiring a translational change in velocity (delta V) of more than 0.3 m/sec. The RCS thrusters are used for smaller maneuvers, and for special instances of attitude control. The RCS thrusters have more control authority than the RWA, and for this reason they are used to control the spacecraft during low altitude Titan flybys, in order to maintain attitude control in the presence of Titan atmospheric torque. The RCS system is also needed to maintain attitude during momentum biases of the RWAs, which are performed periodically to optimize the RWA momentum vector to minimize wheel rate regimes that are deemed unhealthy. The RWA subsystem controls the attitude for most other situations, as it provides more stable and precise pointing control, and does not consume hydrazine.

II. Cassini Reaction Control Subsystem Description

Cassini has two independent branches of monopropellant hydrazine RCS thrusters[1], a prime and offline backup, each capable of providing translational velocity changes and maintaining complete 3 axis control. The arrangement of the thrusters with respect to spacecraft coordinates is shown at left in Fig 1.

The RCS thrusters are separated into four clusters based on location, such that the A-branch thrusters are essentially collocated with their corresponding B-branch thrusters. Each thruster has a pair of redundant catalyst bed heaters (CBH), with temperature sensors located at the thruster inlets and catalyst bed heater locations. The A-branch Z-facing thrusters have combustion chamber pressure sensors, a feature that is unique for monopropellant thrusters of this size.

The Z-facing thrusters are not coupled, so usage of these thrusters for attitude control imparts a translational change in velocity that must be accounted for in the trajectory design.

Both 'A' and 'B' branches share the same helium pressurized monopropellant hydrazine fuel tank, which made use of a single helium pressurant recharge bottle in 2006. The system is not regulated, and has been operating in blow down mode ever since. Downstream of the helium pressurized hydrazine tank, the system is entirely redundant. Both thruster branches are isolated from the pressurized hydrazine tank via latch valves (LV), with LV 40 set to open at launch for the 'A' branch, and LV 41 closed at launch, such that the 'B' branch thrusters remained unused (see Fig 2). The 'A' branch was designated the prime branch at launch. The intention was to keep branch 'B' as an unused, dedicated backup.

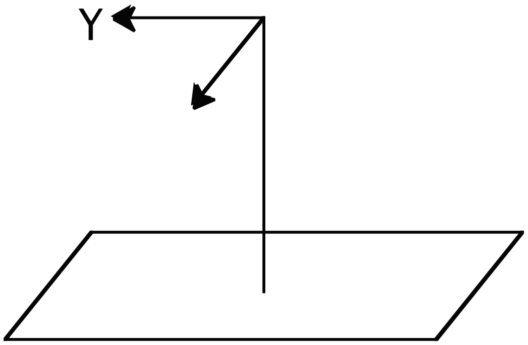


Figure 1. Cassini RCS Thruster Orientation.

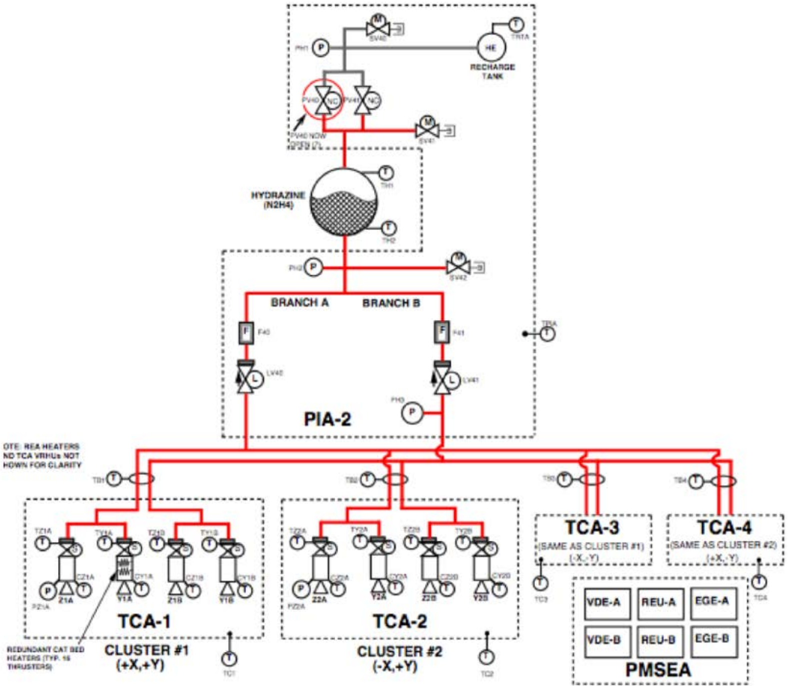
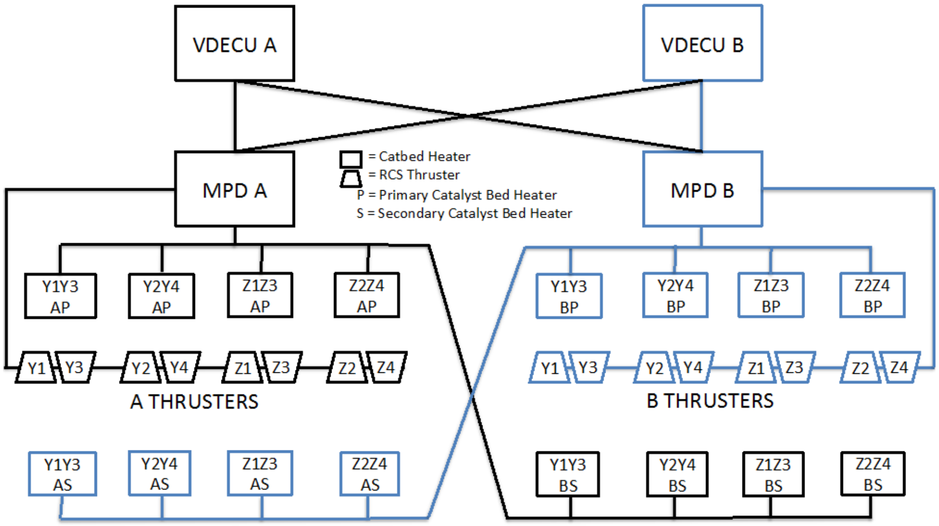


Figure 2. Cassini RCS Schematic[2]

The RCS hardware consist of redundant cross strapped Valve Drive Electronics Control Units (VDECU) and Mono-prop Drivers (MPD), which control the thruster valves, required catbed heaters, as shown in figure 3. MPD A controls latch valve 40 for the 'A' Branch, and MPD B controls LV 41 for the 'B' branch.



Current FSW designated prime shown in blue

Figure 3. RCS Hardware Driver Block Diagram

In October 2008, two of the eight A-branch RCS thrusters, which had been used flawlessly since launch for 11 years as the prime set, began to show signs of degradation.[3] One of the recommendations from the Cassini propulsion team was an in-flight swap to the backup thruster B-branch, because this branch had never been used in flight, and thus had pristine thrusters and catalyst beds. The swap to the 'B' thruster branch was completed in flight over the course of nine days in March 2009.[2] Cassini continues to operate flawlessly on the B-branch, but if degradation occurs on any of the thrusters in this branch, we may be forced to adopt a "mixed" branch configuration, with some of the A-branch thrusters being used with some of those from the B-branch.

III. Problem with AACS Fault Protection In "Mixed Mode"

The Cassini attitude control flight software is capable of supporting such a "mixed" thruster configuration. All that is needed is to designate which set of thrusters on these two thruster branches is prime. The original fault protection logic, however, was not capable of properly handling a mixed branch configuration. The AACS FSW version A8.8.0 was recently updated to improve the FP handling of thruster faults in the mixed branch configuration. This new version was called A8.9.0.

If a thruster leak is detected in a mixed thruster configuration, the fault protection logic of the old Cassini flight software (version A8.8.0) will swap to an "all B branch" thruster configuration and close the A-branch latch valve (LV40). This is the correct response if the leaky thruster is from the A-branch. If, however, the leaky thruster is from the B-branch, the current "all B-branch" fault protection response will not shut off the monopropellant latch valve associated with the problematic thruster, and the fault will not be mitigated. Hydrazine will be still leaking out of the leaky B-branch thruster.

This limitation of the A8.8.0 flight software build was rectified in the A8.9.0 flight software build (that was uploaded on the Cassini spacecraft on December 12, 2012). The new fault protection logic design (for mixed thruster configuration) is described in this paper.

IV. Design of Mixed Branch Fault Protection

Although the Cassini fault protection design is not required to be tolerant to multiple failures, provisions should be made in the event of reasonable and recoverable future failures of the thruster system. No design provisions are made for failure modes which Cassini lacks the hardware redundancy to mitigate. An example of which would be permanent thruster leaks on both thruster branches. In the event of a leak on both thruster branches, or a failure of both mono-propulsion drivers (MPDs), orbit maintenance will not be possible and the mission science will not be possible. Additionally, the fault protection design has assumed that there is no more than a single "hard" thruster failure per thruster branch, where a hard thruster failure is defined as complete loss of thrust. Partial thrust degradation (such as exhibited by the Z3A and Z4A thrusters) is acceptable and recoverable.

Autonomous detection of a leaking hydrazine thruster was of particular importance to the Cassini mission due to the risk of the wasting vital hydrazine propellant after a leak occurs. Early in the mission, communication with Cassini occurred only once per week. Other critical periods where delayed leak detection was considered especially threatening were the approach to the Earth flyby in August 1999 and during Saturnian tour operations. The Cassini fault protection design includes three leak detection error monitors, one for each spacecraft body axis, which monitor for excessive thruster commanding (ETC). These monitors compare expected angular momentum accumulation with estimates of commanded RWA and RCS control quantities. If deviations rapidly accumulate, a leak detection error monitor will trigger and fault protection response will occur (see Reference 4).

In response to an excessive thrusting error, the onboard fault protection will attempt a number of corrective actions including swapping to the backup sun sensor assembly (SSA), stellar reference unit (SRU), inertial reference unit (IRU), valve driver electronics control unit (VDECU), backup thruster branch, and calling system Safing. The appropriate corrective action is selected based upon a tier count parameter which increments each time an excessive thrusting condition is detected. At a high level, the pre-AACS FSW 8.9.0 FP design takes the actions described in table 1.

Table 1: Pre AACS A8.9.0 FSW Fault Protection Behavior

Tier	FP Action Taken	Relevant Parameters which govern FP behavior
1	Reset monitors, request System Safing	
2	Reset monitors, request System Safing	
3	Reset monitors, request System Safing	
4	Reset monitors, request System Safing	

5	Reset monitors, request System Safing	
6	Swap thruster branches*, reset monitors, request System Safing	Swap_Thrusters_2n = 6
7	Swap VDECU, reset monitors, request System Safing	Swap_VDECUs_2n = 7
8	Swap IRU, reset monitors, request System Safing	Swap_IRUs_2n = 8
9	Swap SRU, reset monitors, request System Safing	Swap_SRUs_2n = 9
10	Swap SSA, reset monitors, request System Safing	Swap_SSAs_2n = 10
11+	Reset monitors, request System Safing	

*After the thruster branch swap a thrusters_swapped flag is set to true and the onboard FP will not swap thruster branches again while that flag is set.

On the 6th tier of the FP response to a excessive thrusting error the onboard fault protection will swap thruster branches and close the latch valve to the backup thruster branch (either LV-40 or LV-41). Following the closure of the appropriate latch valve, the FP will issue a 7PAUSE DROP command, which will force AACS to drop inertial attitude knowledge and reacquire attitude knowledge using the updated prime suite of sensors, actuators, and related hardware. Figure 4 illustrates the Cassini AACS mode transition diagram and the applicable transitions between modes.

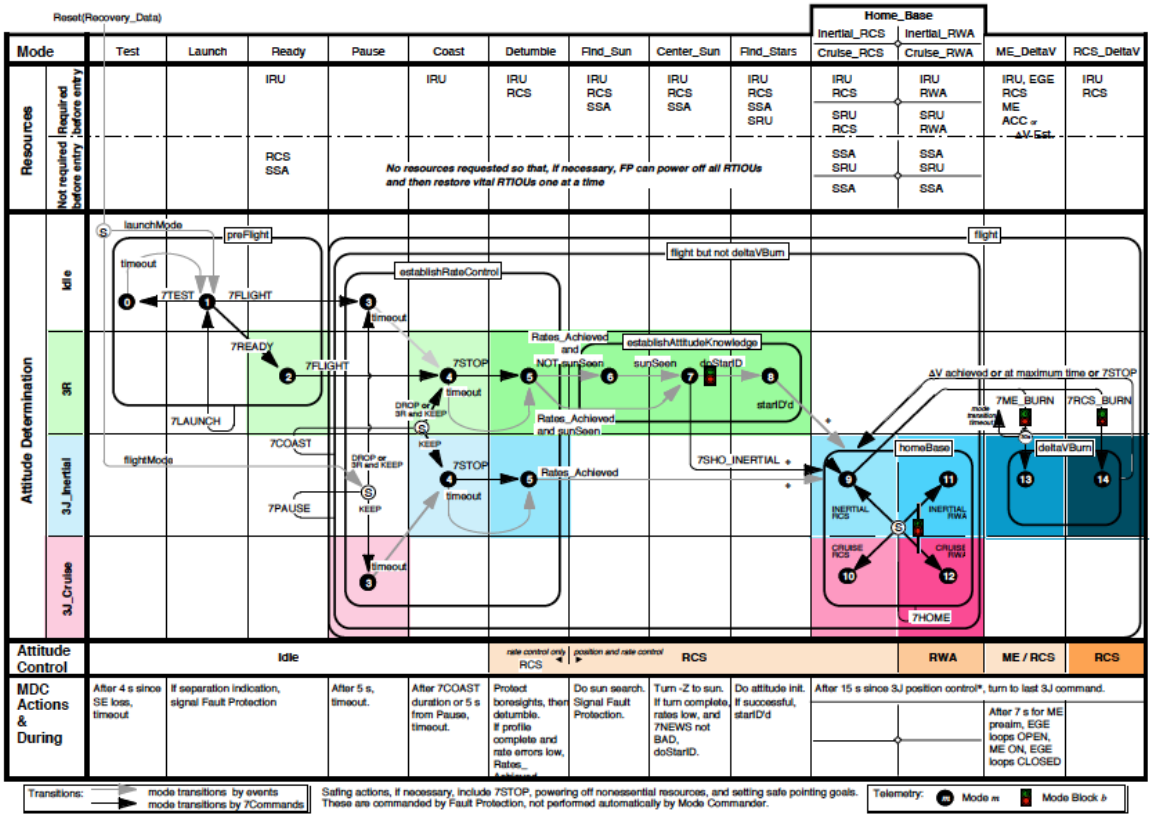

Reset(Recovery_Data)
Home_Base
Mode
Test
Launch
Ready
Pause
Coast
Detumble
Find_Sun
Center_Sun
Find_Stars
Inertial_RCS
Cruise_RCS
Inertial_RWA
Cruise_RWA
ME_DeltaV
RCS_DeltaV
Resources
Required before entry
Not required before entry
IRU
IRU
IRU
RCS
IRU
RCS
SSA
IRU
RCS
SSA
IRU
RCS
SSA
SRU
IRU
RCS
SRU
RCS
SSA
SRU
SSA
IRU
RWA
SRU
RWA
SSA
SRU
SSA
IRU, EGE
RCS
ME
ACC or ΔV Est.
IRU
RCS
RCS
SSA
No resources requested so that, if necessary, FP can power off all RTIOUs and then restore vital RTIOUs one at a time
Attitude Determination
Idle
3R
3J_Inertial
3J_Cruise
launchMode
preFlight
flight
flight but not deltaVBurn
establishRateControl
timeout
7TEST
7FLIGHT
7READY
7FLIGHT
7LAUNCH
7COAST
7PAUSE
flightMode
DROP or 3R and KEEP
DROP or 3R and KEEP
KEEP
KEEP
7STOP
7STOP
timeout
Rates_Achieved and NOT sunSeen
establishAttitudeKnowledge
sunSeen
doStarID
starID'd
Rates_Achieved and sunSeen
Rates_Achieved
7SHO_INERTIAL
ΔV achieved or at maximum time or 7STOP
7ME_BURN
7RCS_BURN
mode transition timeout
homeBase
deltaVBurn
INERTIAL RCS
INERTIAL RWA
CRUISE RCS
CRUISE RWA
7HOME
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
S
Attitude Control
Idle
rate control only
RCS
position and rate control
RCS
RWA
ME / RCS
RCS
MDC Actions & During
After 4 s since SE loss, timeout
If separation indication, signal Fault Protection
After 5 s, timeout.
After 7COAST duration or 5 s from Pause, timeout.
Protect boresights, then detumble. If profile complete and rate errors low, Rates_Achieved
Do sun search. Signal Fault Protection.
Turn -Z to sun. If turn complete, rates low, and 7NEWS not BAD, doStarID.
Do attitude init. If successful, starID'd
After 15 s since 3J position control*, turn to last 3J command.
After 7 s for ME preaim, EGE loops OPEN, ME ON, EGE loops CLOSED
Transitions:
mode transitions by events
mode transitions by 7Commands
Safing actions, if necessary, include 7STOP, powering off nonessential resources, and setting safe pointing goals. These are commanded by Fault Protection, not performed automatically by Mode Commander.
Telemetry:
Mode m
Mode Block b

Figure 4. Cassini AACS Mode Transition Diagram[5]

Closing the upstream latch valve will stop a thruster leak and is the appropriate corrective action, but the challenge is to determine which latch valve to close. Additionally, the on-board FP will not swap thrusters a second time after it swaps for the first time. Three main design change options were considered to protect against a leaky thruster while in a mixed thruster configuration.

The first option considered was to close both upstream latch valves LV-40 and LV-41 to isolate all thruster leaks on both thruster branches and transition to a new RWA-based Safing mode. This provides robust mitigation to the widest range of thruster failures, but requires significant amount of design changes and testing. The AACS design which has undergone thorough testing and has been stable with over fifteen years of flight experience, always uses the RCS control system to detumble the spacecraft (bring body rates under control), find the sun, point to the sun, find stars (to re-establish 3-axis attitude knowledge) and finally slew to a “safe” attitude (typically HGA to Sun with SRU pointing at an unobstructed star field) to allow communication with ground controllers. The AACS design does not have the capability to perform these actions under RWA control. Significant re-design work would be required to establish an RWA-based recovery path. Additionally, the analysis and testing involved to ensure that the RWA system can always achieve these goals under a range of credible non-zero system momentum conditions would be difficult to bound. Given the low likelihood of a thruster leak scenario, the implementation complexity, and the relatively robust quantity of hydrazine remaining onboard, the option to close both LV-40 and 41 and use RWA control was not selected to mitigate the vulnerability to a leak while in mixed thruster branch operation.

The second option considered was to design the fault protection to diagnose which thruster is leaking, close the latch valve on that leaking thruster branch, and recover via the nominal RCS-based Safing design with the other branch of thrusters. This method maintains the same tiering for the subsequent tier count of the retry_attitude_initialization response, but it requires logical changes to the diagnosis step of the activation rules and a modification of the retry_attitude_initialization response. Furthermore, there are concerns about the accuracy of the diagnosis being able to uniquely and unambiguously determine which thruster is leaking. The complexity of the required design and the risk of a false diagnosis being fatal led us away from this option.

The last option is the simplest, and is the one implemented in the AACS A8.9.0 FSW build. Swap thruster branches twice, if needed, instead of the baseline one time. This required a modification of internal count parameters and minor logic changes to the swap thrusters response, in order to close LV-40 and swap to the B-branch thrusters on the 6th tier of FP action, and to open LV-40 and close LV-41 and swap to the A-branch thrusters on the 7th tier of FP action. In the event of a thruster leak on branch B, fault protection actions will swap to an all B-branch set of thrusters on the 6th tier of the response. This action will not mitigate the thruster failure in this case, but the next tier (7th tier) of FP actions will swap to the A-branch thrusters, and close LV-41, which will mitigate the thruster leak. In the event of a thruster leak on branch A, the FP actions will swap to an all B-branch set of thrusters on the 6th tier of the response and mitigate the leak.

Table 2: AACS A8.9.0 FSW Fault Protection Behavior

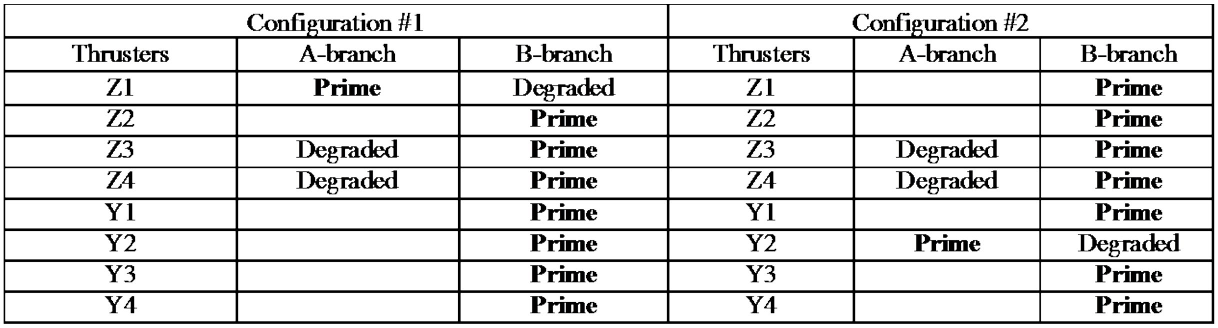
Tier	FP Action Taken	Relevant Parameters which govern FP behavior
1	Reset monitors, request System Safing	
2	Reset monitors, request System Safing	
3	Reset monitors, request System Safing	
4	Reset monitors, request System Safing	
5	Reset monitors, request System Safing	
6	Swap thruster branches, reset monitors, request System Safing	Swap_Thrusters_2n = 6
7	**Swap thruster branches a second time**, reset monitors, request System Safing	
8	Swap VDECU, reset monitors, request System Safing	Swap_VDECUs_2n = **8**
9	Swap IRU, reset monitors, request System Safing	Swap_IRUs_2n = **9**
10	Swap SRU, reset monitors, request System Safing	Swap_SRUs_2n = **10**
11	Swap SSA, reset monitors, request System Safing	Swap_SSAs_2n = **11**
12+	Reset monitors, request System Safing	

Although the selected option to swap thruster branches twice requires the least code modification, there are some drawbacks from a hydrazine usage perspective. In the event of a thruster leak on the A-branch thrusters, it takes the on-board fault protection an additional tier of response to mitigate the thruster leak. As described in reference 4, the excessive thruster commanding error monitor uses the Euler equation to detect unexpected accumulation of angular momentum (which is diagnosed as a thruster leak). Based on the design of the monitor and the onboard threshold, the additional hydrazine lost by not mitigating a B-branch thruster leak until the 7th tier, as compared to the 6th tier, was determined to be insignificant.

V. Mixed-branch RCS Fault Protection Test Design

Every time an update is planned to the AACS FSW, an extensive amount of testing is performed on multiple platforms to verify the proper design and implementation of the update. In addition to the standard acceptance and regression tests that are performed for every new version of FSW, new test cases were designed that specifically targeted the mixed branch FP changes that were made for FSW version A8.9.0. We wanted to stress the system, looking for possible weaknesses in the design and implementation, whereby undesirable fault responses might occur in the presence of multiple or extremely unlikely faults. In other words, we wanted to test the boundaries and limitations of the system.

The first thing considered in the design of the test suite was the configuration of the spacecraft to be used in the tests. Since Cassini has a total of 16 RCS thrusters from which a subset of 8 are used at any one time (see figure 1), it would be virtually impossible to perform every test with every possible permutation of mixed branch thruster configuration. We chose to make use of three mixed branch thruster configurations (see table 3) in our testing, making sure to include an intelligent representation of Z thrusters, because they are unbalanced, and Y thrusters, because they are balanced (see figure 1).



Configuration #1			Configuration #2		
Thrusters	A-branch	B-branch	Thrusters	A-branch	B-branch
Z1	**Prime**	Degraded	Z1		**Prime**
Z2		**Prime**	Z2		**Prime**
Z3	Degraded	**Prime**	Z3	Degraded	**Prime**
Z4	Degraded	**Prime**	Z4	Degraded	**Prime**
Y1		**Prime**	Y1		**Prime**
Y2		**Prime**	Y2	**Prime**	Degraded
Y3		**Prime**	Y3		**Prime**
Y4		**Prime**	Y4		**Prime**

Table 3. Mixed Branch Thruster Configurations Used in Testing

The reader will remember that the A branch Z3 and Z4 thrusters have degraded in flight[3], which is why both of the test configurations make this assumption. The configurations are intentionally biased toward having most of the B branch thrusters designated as FSW prime, since this is the most likely scenario, given that that A branch thrusters have seen the most use in flight.

As for the spacecraft mass properties and thrust values to use in testing, we decided to use the values predicted for the year 2015, since this is half way between the present time and the end of the mission, in 2017. All other spacecraft hardware states such as RWA configuration, propulsion latch valve positions, star tracker and sun sensor power states, etc., set to match the current operational state of the spacecraft.

Once the set of test configurations was defined, individual test cases were designed to make sure the software change performed as expected in various nominal operational scenarios, as well as with the introduction of realistic and extreme faults.

A description of some of the fault protection test cases, along with the objectives of performing these sets of tests are explained below:

1. A- or B-branch RCS thruster is stuck open or closed. The objective of performing this set of test cases is to verify that the on-board FP design will switch to the thruster branch without the stuck open (or closed) thruster. Moreover, the LV (LV-40 or LV-41) for the thruster branch with that stuck open/closed thruster is commanded closed, to stop the leak in those stuck open test cases.
2. VDECU, MPD, or LV faults. Determine that the on-board FP design will replace the failed MPD (or VDECU or LV) using its backup. Thereafter, the failed equipment is powered off.
3. RWA fault. Verify that the on-board FP design will transition from the Inertial_RWA to Inertial_RCS attitude control mode in the presence of a permanent RWA fault. Thereafter, the mixed-branch thruster set will slew the S/C to an Earth-pointed attitude. All RWAs are powered off. But both MPDs (which are needed for the mixed-branch RCS thruster configuration) will stay powered on.
4. Non-AACS Fault Induced Safing. Verify that after an AFC reset, the FSW designated prime states of the thruster configuration (thrusters, CBH, MPD, and VDECU) will be maintained via the recovery data. FP will successfully slew the S/C to the Safing attitude using the mixed-branch thrusters. Both MPD (that are needed for the mixed-branch RCS thruster configuration) will stay powered on.

5. Catbed Heater Fault. Confirm that the on-board FP design will successfully replace the faulted prime CBH using their secondary counterparts.
6. Attitude Determination Functional Failures. These test cases are all members of the FP regression test set. They check out several safety net response scripts. The objective of this set of test cases is to ascertain that actions taken by these scripts could be supported by a mixed RCS thruster configuration.

VI. Test Implementation

The AACS team made use of two hardware platforms for testing the new version of the FSW, with hundreds of test cases emphasizing regression and new functionality. Both platforms have advantages and disadvantages. The AACS team members used discretion in assigning the proper test case to the proper test environment.

A. Cassini Test Platforms

The two main test platforms available to the AACS engineers are the Flight Software Development System (FSDS) and the Integrated Test Laboratory (ITL).

FSDS is a workstation-based simulation without any hardware in the loop[7]. It runs a compiled version of the FSW, with all the hardware and environmental inputs simulated. It runs relatively quickly, approximately 8 times real time, and can be scripted with multiple instances running at the same time. The scripting capability allows for easy repeatability and updating of tests, which makes regression testing of new versions of FSW much easier to design, execute, and evaluate. The use of a tool like FSDS allowed us to run and evaluate hundreds of test.

The ITL is a very high fidelity system mode integrated hardware test facility, with the AACS FSW running on a flight spare Avionics Flight Computer (AFC), and multiple flight spare avionic hardware units in the loop[8]. The ITL platform is very flight like, and as such is very resource intensive. It can only run one test at a time in real time, and takes several hours to boot up and prepare each test. This effectively limited us to a few dozen tests performed in the ITL.

B. Interesting Results

First and foremost, the results of the testing showed the mixed branch fault protection design and implementation to be a success. It is robust and effective in isolating thruster leaks quickly, without causing unnecessary thruster swaps in response to faults that are not thruster related, in the vast majority of cases. Regardless of the initial thruster configuration, the spacecraft proved capable of recovering from a hydrazine leak by isolating the faulted thruster branch and continuing operation on the spare branch.

There were extreme scenarios, however, whereby unexpected or undesirable results occurred, but they were deemed so unlikely, or there are operational workarounds to mitigate their effects, that further changes to the FSW was not necessary.

1) Phantom Momentum Induces False Excessive Thruster Commanding Fault Trip

In extreme fault cases, a known mismatch between the FSW modelled RWA momentum and the actual momentum can occur, when the RWA system is unexpectedly powered off, whether from a safing response, or from an AFC reset[6], as shown in figure 6. This mismatch in momentum can induce the Excessive Thruster Commanding (ETC) Fault Monitor to erroneously trip, as it uses the Euler equation to monitor spacecraft rotation[4]. The design of the mixed branch thruster fault protection is to delay the ETC swap of thruster branches to the fifth tier to allow time for the phantom momentum to decay, so that the thruster branch is not swapped unnecessarily. This was thought to be sufficient margin, so that a thruster swap would not occur due to ETC

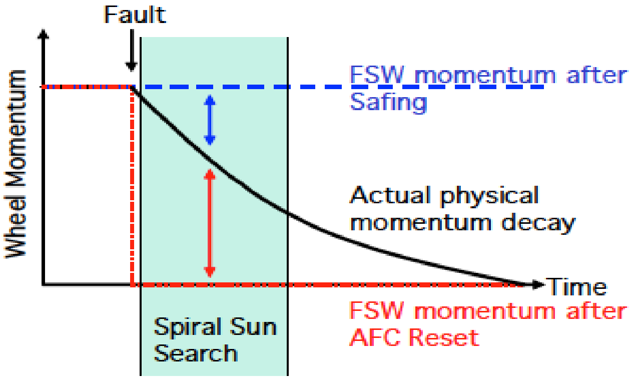

Fault
Wheel Momentum
FSW momentum after Safing
Actual physical momentum decay
Time
FSW momentum after AFC Reset
Spiral Sun Search

Figure 6. Graphical Concept of RWA FSW Phantom Momentum[6] *Illustrates two scenarios of FSW discrepancy. Blue arrow discrepancy occurs when a Safing or FP-related RWA to RCS transition is invoked, red arrow discrepancy occurs when an AFC reset is invoked.*

responding to phantom momentum, but would still occur quickly enough in response to a real thruster leak.

This proved not to be the case, however, for a few extremely unlikely worst case instances of phantom momentum. One such case involved the spacecraft initially anti-sun pointed, with an induced AFC reset with loss of attitude knowledge and maximum possible RWA momentum. This induced a sun search with the maximum amount of phantom momentum possible. In this case, ETC tripped 6 times and induced an unnecessary thruster branch swap. In flight, operations rules and ground software prevent such a large amount of initial momentum on the RWAs, so the test case is deemed extremely unlikely to occur in flight. Regardless, it would not be catastrophic if it did occur, as the operators would simply command a swap back to the original thruster configuration. Since the undesired response was not catastrophic and is extremely unlikely to occur, we decided to leave the FSW unchanged, even though the original design intent was not completely satisfied under every circumstance.

2) Interfering Fault Responses

The AACS Fault Protection is object oriented, where multiple response scripts can be active at one time[5]. In the process of testing the mixed branch FSW update, we found a scenario whereby two response scripts interfere with one another in an undesired way. The ETC error monitor is supposed to allow for five trips of its momentum threshold before the response script swaps thruster branches in an attempt to isolate a suspected thruster problem. The FP software did not respond in the expected manner, however, when it came to a few particular test cases involving stuck closed thrusters.

In a test case involving a stuck closed Z1A thruster valve during change to the RWA momentum in RCS control, it turned out that the Excessive Thruster Commanding fault monitor tripped nine times before commanding a swap to the B-branch, which isolated the stuck closed thruster and remediated the fault. This occurred because another fault monitor, Excessive Attitude Error, was also tripping its threshold, and the two monitors share a common tier count parameter. Both monitors were overwriting the counter, so ETC actually tripped more than the design number of times before the thruster swap.

We were never able to cause this situation to occur in the many stuck open test cases we ran. Since a stuck closed thruster does not leak hydrazine, the extra tiers exercised before the thruster swap was not deemed a serious problem, and we decided against making further updates to the FSW.

3) Safety Net Fault Protection Responses

The test cases involving “safety net” Fault Protection responses provided results that proved challenging. Safety net Fault Protection responses like “Long Sun Search”, “Suspend Attitude Control”, and “Pause and Safe” are routines that react when lower level fault protection are unable to mitigate faults. Due to this design, excessive swapping of hardware will occur prior to fault mitigation if the remedy comes from these higher order responses. From a testing standpoint, when the engineer recognizes swapping thruster branches will cure the fault, a swap of IRUs or SRUs prior to mitigating the fault may be considered unnecessary. However, Fault Protection was architected such that lower level FP attempts all necessary hardware combinations prior to attempting substantial response actions like swapping primeness of the thruster branch set. A handful of test cases fell into extraneous hardware swapping; but since the fault was mitigated as intended, those test cases passed their success criteria.

VII. Conclusion

The successful design, implementation, and testing of the update to Cassini’s mixed RCS branch AACS Fault Protection Flight Software was a huge undertaking, the success of which required the collaboration of many talented individuals. This paper describes the challenges of designing and testing this update. Although the FSW has been successfully uplinked and is currently operating on board the spacecraft, several important lessons were learned along the way.

Future missions that make use of dual string propulsions systems would do well to take advantage of that fact in all aspects of the FSW. The Cassini AACS FSW was originally designed to properly handle a mixed branch propulsion configuration for nominal operations, but the fault protection software was not designed to handle this possibility gracefully. Much time and energy could have been saved if the mixed branch capability had been incorporated into the fault protection software at launch.

We found a few cases where a lack of strict adherence to the object-oriented paradigm caused unexpected results. The phantom momentum case had been known and published previously[5], but the fault monitor counter interference case was not. Future missions would do well to implement strict controls on maintaining the object-oriented methods of data scope enforcement.

The scripting capability of the Flight Software Development System proved invaluable in the testing and verification of the new FSW. Individual test cases were easily modified and the results were easily evaluated, as they could be quickly run and compared to the results from previous versions of the FSW. This capability is especially valuable on a long term project like Cassini, where the knowledge base loss from inevitable turnover in personnel is mitigated by the repeatable nature of scripted tests. Not all missions have such a test platform, but our experience with Cassini shows it to be a valuable and cost effective method for thorough testing of a complicated system.

Acknowledgments

The authors are grateful to many people, without whose help and inputs, this paper could not be written: Juan Hernandez, Todd Barber, Tom Burk, Sima Lisman, and Julie Webster, among others.

The work described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration.

References

[1]Barber, T.J. and Cowley, R.T., "Initial Cassini Propulsion System In-Flight Characterization", AIAA-2002-4152. 38th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit, Indianapolis, Indiana, July 7-10, 2002.

[2]Bates, David M., "Cassini Spacecraft In-Flight Swap To Backup Attitude Control Thrusters," *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, Toronto, Canada, August 2-5, 2010.

[3]JPL Cassini-Huygens Mission Status Report (February 2, 2009). http://www.jpl.nasa.gov/news/news.cfm?release=2009-014.

[4]Lee, A.Y., "Model-based Thruster Leakage Monitor for the Cassini Spacecraft," *Journal of Spacecraft and Rockets*, Vol. 36, No. 5, pp. 745-749, September-October, 1999.

[5]Brown, Jay, "Cassini Attitude Control Flight Software: From Development to In-flight Operation," *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, Honolulu, HI, August 18-21, 2008.

[6]Brown, G. Mark, "An Overview of the Fault Protection Design for the Attitude Control Subsystem of the Cassini Spacecraft," *Proceedings of the American Control Conference*, Philadelphia, Pennsylvania, June, 1998.

[7]Brown, J., Lam, D., "The role of the Flight Software Development System simulator throughout the Cassini mission," *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, San Francisco, CA, August 15-18, 2005.

[8]Badaruddin, Kareem S., "Creative Solutions to Cassini's Testing Challenges," *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, San Francisco, CA, August 15-18, 2005.