

Cassini Attitude Control Fault Protection Design: Launch to End of Prime Mission Performance

Peter C. Meakin¹

Jet Propulsion Laboratory, California Institute of Technology, Pasadena CA 91109

The Cassini Attitude and Articulation Control Subsystem (AACS) Fault Protection (FP) has been successfully supporting operations for over 10 years from launch through the end of the prime mission. Cassini's AACS FP is complex, containing hundreds of error monitors and thousands of tunable parameters. Since launch there have been environmental, hardware, personnel and mission event driven changes which have required AACS FP to adapt and be robust to a variety of scenarios. This paper will discuss the process of monitoring, maintaining and updating the AACS FP during Cassini's lengthy prime mission as well as provide some insight into lessons learned during tour operations.

Nomenclature

<i>AACS</i>	=	<i>Attitude and Articulation Control Subsystem</i>
<i>AFC</i>	=	<i>AACS Flight Computer</i>
<i>ATC</i>	=	<i>Autonomous Thermal Control</i>
<i>CAIP</i>	=	<i>Constraint Avoidance in Progress</i>
<i>EGA</i>	=	<i>Engine Gimbal Assembly</i>
<i>EM</i>	=	<i>Error Monitor</i>
<i>EOPM</i>	=	<i>End of Prime Mission</i>
<i>ETC</i>	=	<i>Excessive Thruster Commanding</i>
<i>FP</i>	=	<i>Fault Protection</i>
<i>FPDD</i>	=	<i>Fault Protection Design Document</i>
<i>FOV</i>	=	<i>Field of View</i>
<i>FSW</i>	=	<i>Flight Software</i>
<i>GSW</i>	=	<i>Ground Software</i>
<i>HWM</i>	=	<i>High Water Mark</i>
<i>IRU</i>	=	<i>Inertial Reference Unit</i>
<i>LAD</i>	=	<i>Last Available Data</i>
<i>MDC</i>	=	<i>Mode Commander</i>
<i>MEVD</i>	=	<i>Main Engine Valve Driver</i>
<i>OTM</i>	=	<i>Orbit Trim Maneuver</i>
<i>RCS</i>	=	<i>Reaction Control System</i>
<i>RWA</i>	=	<i>Reaction Wheel Assembly</i>
<i>SEU</i>	=	<i>Single Event Upset</i>
<i>SID</i>	=	<i>Star Identification</i>
<i>SOI</i>	=	<i>Saturn Orbit Insertion</i>
<i>SSA</i>	=	<i>Sun Sensor Assembly</i>
<i>SSPS</i>	=	<i>Solid State Power Switches</i>
<i>SRU</i>	=	<i>Stellar Reference Unit</i>
<i>TCA</i>	=	<i>Titan Closest Approach</i>
<i>TVC</i>	=	<i>Thrust Vector Control</i>
<i>XM</i>	=	<i>Extended Mission</i>

¹ Cassini AACS Fault Protection Lead, Jet Propulsion Laboratory, 4800 Oak Grove Drive, Pasadena California 91109, USA. Peter.C.Meakin@jpl.nasa.gov.

I. Introduction

THE Cassini spacecraft is a 3-axis stabilized zero momentum spacecraft using reaction wheel assemblies (RWAs) for fine science pointing and a reaction control system (RCS) for maneuvers, RWA momentum management and periods requiring high control authority. The RCS is comprised of 16 MR-103 0.9 N thrusters, in two branches of 8 thrusters. The Cassini spacecraft, now orbiting Saturn, was launched on October 15, 1997 on a Titan IVB launch vehicle. After a nearly 6.7 year cruise Cassini performed the Saturn Orbit Insertion (SOI) burn on June 30, 2004. Following SOI is the 4 year prime mission science tour of the Saturnian system. The Cassini prime mission ended July 2 2008, with an extended mission (XM) approved through Sep 30, 2010.

During tour operations, Cassini experiences varied orbit inclinations from equatorial to nearly 75 degrees. There are 44 Titan flybys during prime mission with 23 low altitude flybys in which Cassini experiences drag torque due to Titan's atmosphere. A total of 146 orbit trim maneuvers (OTMs) were planned during tour operations with only 102 maneuvers were executed during the tour operations and 19 TCMs executed during cruise. Thrust vector control (TVC) during main engine maneuvers is performed by the main engine gimbal, during small RCS maneuvers the 4 Z-facing thrusters are off-pulsed to maintain the spacecraft attitude during the burn.

When launched, the Attitude and Articulation Subsystem (AACS) Fault Protection (FP) design, while adequate for 6.7 years of cruise, was not yet complete for several critical mission events. Significant architecture and algorithm design changes were made during the cruise, and numerous parameter changes have been made during tour. This paper will discuss the FP performance during Cassini's prime mission and suggest some of the numerous lessons learned.

II. Brief Overview of AACS FP Architecture

The topic of Cassini AACS FP design extends beyond FP software algorithms, FP design begins at the hardware level. The AACS utilizes fully block redundant hardware except for the single string accelerometer which is used during main engine maneuvers. In the case of the accelerometer a burn timer is used as a software backup. AACS algorithms and processing occurs on the dedicated GVSC 1750A AACS Flight Computers (AFCs). Significant cross strapping exists throughout the AACS hardware. Figure 1 shows a block diagram of the AACS hardware including the cross strapping.

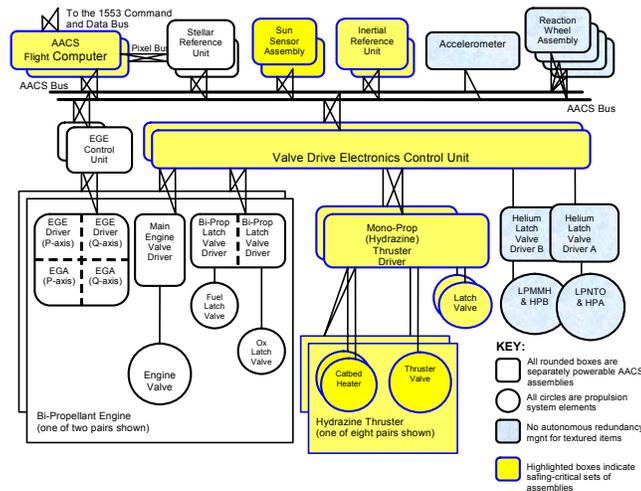


Figure 1. AACS Block Diagram Attitude control sensor and actuator block diagram displaying cross-strapping. (from ref. 3)

In order to understand the modifications made to FP error monitor's thresholds and design, a basic understanding of the Cassini AACS FP software algorithms and design is necessary. Detailed descriptions of the Cassini AACS FP design are described in a series of papers published at the 1998 American Control Conference^{3,6}. The AACS FP design is complex, containing 317 error monitors, 310 activation rules and 221 response scripts. A partial list of the driving AACS FP requirements include: AACS shall be tolerate to any single permanent fault, tolerate of environmentally-induced transient errors, tolerate a power outage of up to 37 milli-seconds, and tolerate faults that

cause invalid commands. A partial list of AACS FP design goals include: locate faults as quickly and accurately as possible, recognize that a single fault may cause multiple errors, tolerate all expected operating scenarios, tolerate residual abnormal condition that may persist following an appropriate fault response, find a natural decomposition of FP algorithms, and recovery from anomalous conditions as easily as possible.

The AACS FP architecture is made up of error monitors (EMs), activation rules, response scripts, repair managers and redundancy managers. Error monitors detect deviations from expected performance, apply discriminating filters and summarize their opinion as a “color”. Activation rules use knowledge of the current hardware configuration along with subsystem goals, to diagnose the source and severity of the problem. After making a diagnosis, activation rules then activate one or more appropriate response scripts. Response scripts restore a safe functional subsystem by issuing the appropriate commands and alert messages, and/or directing the actions of the repair managers. Repair managers apply corrective actions to individual physical assemblies, and provide response scripts with repair histories for individual physical assemblies. Redundancy managers coordinate and track prime set changes. Refer to Figure 2 for a block diagram of the AACS FP architecture.

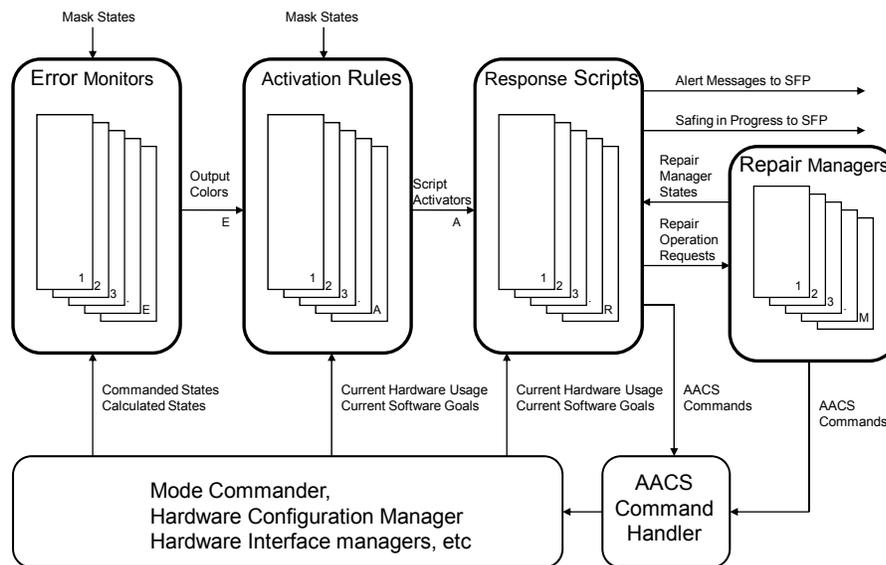


Figure 2. AACS FP Architecture Block Diagram *Figure depicting the AACS fault protection block diagram and the interactions between the various elements of the FP architecture. (from ref. 3)*

Error monitors are embedded throughout Cassini AACS FSW at three levels. There are low-level FP EM which monitor the hardware interface managers. These EMs detect the majority of faults and can usually provide the fault’s location. Low-level EMs are usually simple hardware tests for example the measured SRU CCD temperature is checked to confirm that it falls within an acceptable temperature range. The next level of EMs are control and estimation EMs. Control and estimation EMs monitor AACS algorithm performance, such as excessive attitude error. The details of these EMs are given in reference 3. Control and estimation EMs do not provide as narrow a fault region as the low level EMs since a number of faults can cause these EMs to trigger. The final level of EMs are the functional tests. Functional test EMs represent the broadest monitoring region and are the last line of defense. Functional tests consist of “timeouts” or “give-ups” and provide little fault location. The fault coverage can be thought of as a pyramid with low level FP as the first line of defense. Faults which are not caught by the low level FP are caught by either the control and estimation EMs or the general functional tests. Roughly speaking there are hundreds of low level FP EMs, tens of control and estimation EMs and about ten functional test EMs.

Upon detecting anomalous behavior, error monitors summarize their opinion as a color: green, yellow, red or black. A green color denotes expected behavior. In this case the error test is consistently within the tolerable bounds. A yellow color denotes anomalous but tolerable behavior. While this is anomalous behavior it does not yet merit immediate FP action. A red color denotes unacceptable behavior. This condition requires immediate FP action (invocation of one or more response scripts). A black color denotes no opinion. An EM will generate no opinion when that the EM is inactive, masked, or that performance is out of reasonable bounds and cannot be trusted. Figure 3 depicts the color generator for an EM.

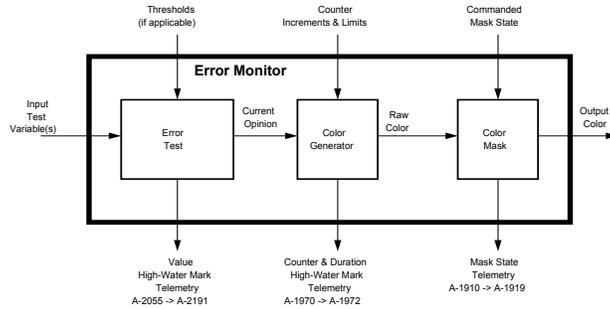


Figure 3. Error Monitor Color Generator Figure demonstrates the discriminating filters and tests applied to the input test before the final color generation.

In order to comply with one of the design requirements and be robust to transient behavior, many AACs EMs utilize a state-space error test. The axes of the state-space error test are known as the *f* and *g*-space. This error test evaluates behavior based on the position in the *error vs rate of change of error* plane to measure expected, tolerable and unacceptable behavior. Generally, errors which are large but quickly reducing are tolerable but still considered anomalous behavior (classified as *g*-space), while errors which are large and growing are unacceptable (classified as *f*-space) and warrant immediate FP action. The details of this approach are given in reference 6 and figure 4. Transient behavior typically introduces a spike in the “*f*-space” EM with little persistence and does not threaten to trigger any *f*-space EMs. In contrast, transient behavior may exceed the *g*-space threshold for a prolonged time.

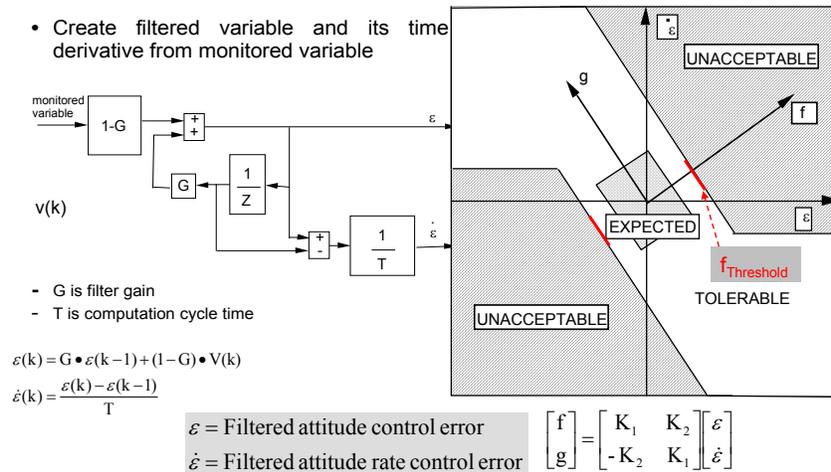


Figure 4. State-Space Error Monitor Tests Figure illustrates the *f* and *g* space error tests employed by many control and estimation error monitors. (from ref. 6)

In order to increase FP robustness, an EM is not triggered unless anomalous behavior persists for a period of time known as the persistence limit. It is not required that the anomalous behavior persist continuously above a FP threshold. Each EM has a distinct increment and decrement count for the persistence limit. Figure 5 depicts the time progression of an error monitor persistence counter. While behavior is unacceptable the persistence counts increase with time at the increment rate. When error test returns to expected (nominal) behavior the persistence count is decreases at the decrement rate. In this way AACs FP will be triggered for intermittent faults which continually exceed the FP threshold and then retreat back into tolerable behavior.

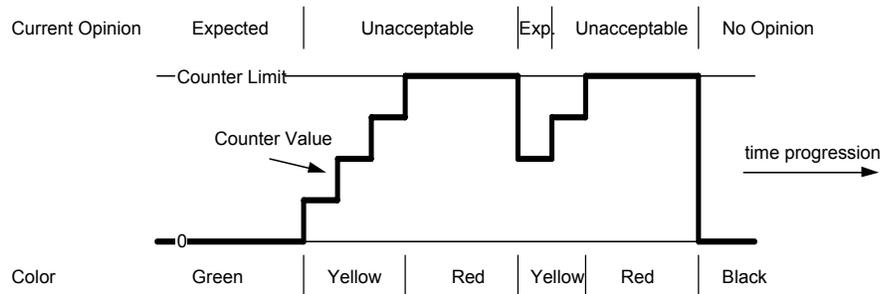


Figure 5. Opinion Generation This figure demonstrates sample EM output color over time.

In addition to the EMs and hardware that comprise FP design, FP design extends to the flight software (FSW) architecture as well. One example of AACS FP embedded in FSW architecture is the mode commander (MDC). AACS employs the MDC to enforce the required resources for attitude estimation and attitude control.¹ Before allowing a transition from the current mode into another mode, the MDC ensures that all of the required resources are available. For example, the FSW prevents a transition to RWA control if the RWAs are unavailable, a transition into main engine ΔV mode if the main engine valve drivers are unavailable. In addition to checking for required resources, the FSW also utilizes “mode blocks” which prevent a transition into a certain mode unless first cleared. These mode blocks serve as a “safety” against accidental mode transitions (such as a transition into the main engine ΔV mode) and is an example of how FP design ensures robustness against commanding errors.

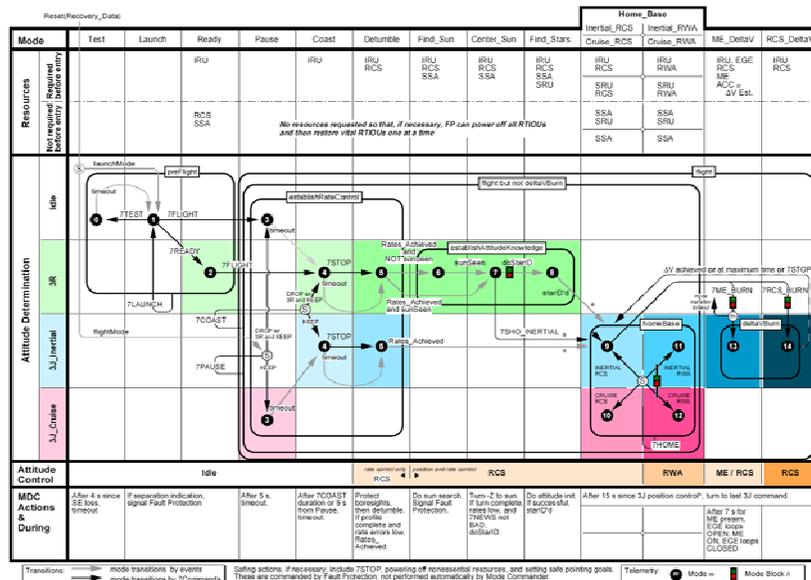


Figure 6. AACS Mode Diagram Mode transition diagram illustrates the required resources for each mode, the allowable mode transitions, and the mode transition blocks.

The AACS FP design can be found in the FSW and hardware design as well as the FP algorithms and EMs executed by FSW. A natural progression ensues where flight hardware and FSW become frozen before FP thresholds and algorithms. Careful FP design in early mission phases helps to ensure that the hardware and FSW design does not preclude certain FP responses or introduce vulnerabilities that FP algorithms cannot mitigate.

III. FP Monitoring and Trending

AACS FP engineers utilize many automated monitoring tools to evaluate the daily FP performance, maneuver performance, and evaluate long term trends in FP error tests. Given the large number of error monitors the variety of FP thresholds and persistence limits, graphical tools are employed to allow FP engineers to quickly determine threatening behavior that does not violate any FP thresholds, and is not recorded in FP event logs or FP telemetry.

AACS FP engineers look for threatening trends in FP performance, proactively checking for hardware, FSW or algorithm degradation. AACS telemetry consists of several thousand channels, many of which provide visibility into FP error tests. Increasing trends in the HWM of error monitor tests could indicate degrading hardware performance (i.e. changing SRU optical focal length, gyro scale factor error drift, increasing RWA viscous drag, etc), degrading algorithm performance (i.e. star catalog proper motion equations deviating away from actual proper motion, TVC controller instability during low tank fill fractions, etc), FSW parameters deviating from physics (i.e. FSW knowledge of mass properties deviating from physical mass properties, FSW thruster magnitude deviating from physical thruster magnitude, etc). Figure 7 illustrates a trend in an increasing particular EM over 14 months. This trend was due to the drifting IRU scale factor error and was later corrected by a FSW parameter update. Although the threshold for this EM was never violated, trending identified a potential future danger where “nominal 3σ behavior” will be perceived by FP as anomalous behavior which merits immediate FP response.

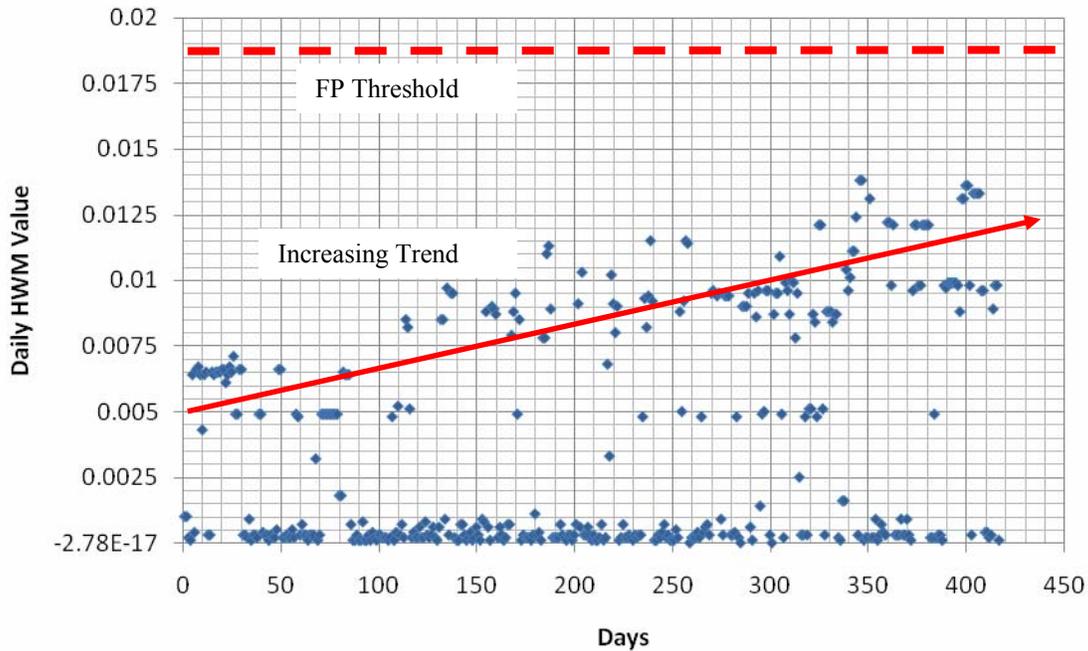


Figure 7. Increasing EM HWM vs Time Chart shows increasing trend in error test HWM over 14 months. Linear trend line illustrates increasing trend in HWM with time.

In addition to the trending performed by AACS FP engineers, a number of daily monitoring scripts are employed to evaluate short term FP performance. One of these AACS monitoring scripts is a daily high water mark (HWM) report. This automated report is generated each day and is distributed as a text report as well as a graphical representation. The graphical representation provides a “quick-look” for AACS FP engineers to evaluate the previous 24 hours of FP performance at a glance. Values are represented as a percent of the FP threshold, $f_{HWM}/f_{Threshold}$. For each EM, the HWM of the previous 24 hours is graphed as red bars, for comparison the previous report’s HWM is displayed as an outlined rectangle. A segment of the HWM report is displayed in Figure 8.

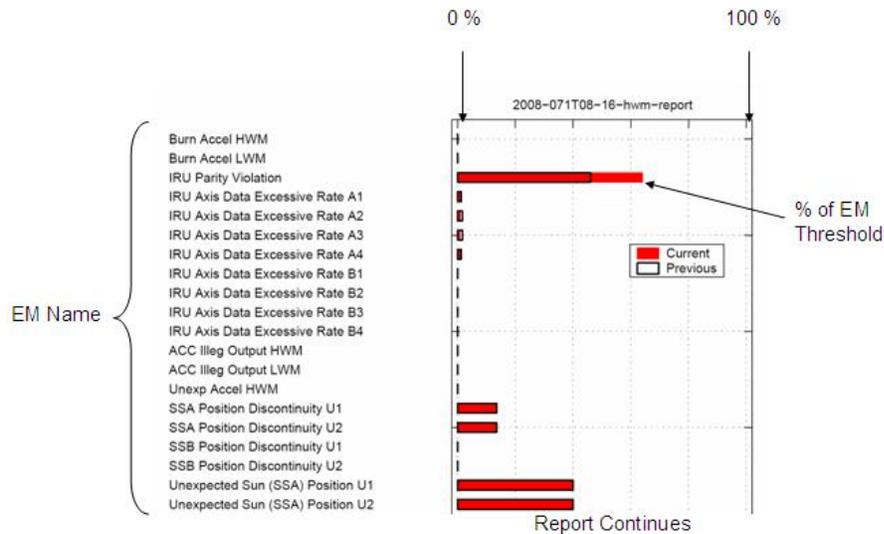


Figure 8. Daily HWM Report *Screen shot from the 2008-071 HWM report. Only a small segment of the report is included. There is a slight increase in the IRU parity violation EM HWM when compared with the previous 24 hour period of time.*

In addition to the HWM report, Cassini FP engineers employ other autonomous AACS monitoring scripts. AACS captures the last available telemetry in the last available data (LAD) reports. The LAD reports capture an instance in time and include many FP counters and telemetry. AACS FP engineers also evaluate FP performance during significant events such as OTMs, flybys or engineering maintenance and calibration activities. These monitoring scripts are employed to help AACS engineers monitor FP performance, any actual violation of FP thresholds or FP action will be captured in “alarmed” telemetry and in the FP event log.

IV. Contributing Factors which Drive FP Changes and Architecture

There are several factors which cause FP to change throughout the mission duration. These factors include environmental, hardware, personnel and mission event changes. The FP architecture was designed with these factors in mind. The AACS FP is highly parametric and easy to tune as needed without requiring logic changes.

A. Environmental Changes

During Cassini’s 11 year mission duration, there have been several environmental changes which have caused FP changes. Changes in the radiation environment, orbital inclination, and proximity to the Sun have all impacted AACS FP. Some of these environmental changes have been expected and proactive action was taken to adapt FP, while others were unexpected and required reactive action to tune FP parameters.

There is a larger flux of high energy protons in Saturn orbit than initially estimated pre-launch. A rate spike is triggered when a high energy proton strikes a gyro, this is called a single event transient (SET). The rate spikes from a SET cause a parity violation which threatens the IRU parity violation error monitor. Occasionally it can also trip the solid state power switches (SSPS) which results in loss of power for a particular assembly, this is known as a single event upset (SEU).⁴ Due to the nearly daily SET-induced IRU parity violations, the persistence limit for the IRU parity violation EM was increased based on flight experience of the SET transient. In this way the AACS FP is robust to SET-induced IRU parity violations without losing sensitivity to detect “real” parity violation, only delaying the response. In response to the SET-induced SSPS trips, FP design requires “graceful” response to the loss of device power. Instead of a “hair-trigger” swap to backup equipment, FP typically power cycles hardware a number of times before becoming exhausted and taking more serious action such as swapping to backup hardware.

Changes in orbital inclination at Saturn orbit necessitate changes in the Safing attitude. While the primary vector remains the same during Tour, the roll about the primary axis, or secondary axis, is not fixed. There are three major considerations in selecting the Safing attitude: bright bodies entering the SRU optical field of view (FOV), control

authority during low altitude Titan flybys, and unacceptable thermal transients on sensitive optics and radiators. Several modifications of the secondary Safing attitude were required during tour to accommodate the changing orbital inclination.

Proximity to the Sun and Earth have impacted several AACS FP design and EM thresholds. During inner solar system cruise, the 4m HGA was used as a sun shield to avoid large thermal load on several science instruments such as the narrow angle camera. In addition to changing Safing attitudes, the sun sensors need to be cognizant of the solar distance. Additionally Cassini requires a large amount of autonomy due to the large one-way light time during tour.

B. Hardware Degradation

Hardware degradation is a concern for all missions, especially for lengthy missions like Cassini. For example, degradation such as increasing RWA viscous friction or hardware changes such as drifting IRU scale factor errors have caused threatening trends such as that depicted in Figure 7. The RWA manager contains a friction estimator based on the RWA rate error and commanded torque. The frictional torque estimate is combined with the attitude commander requested torque to create the total torque request. If the frictional torque request exceeds a reasonable amount than the torque is truncated to a maximum allowable RWA drag limit parameter known as the drag torque compensation limit. The drag torque compensation limit parameter exists to protect against a RWA tachometer failure, or a divergence of the friction estimator. As the viscous torque increases, nominal drag conditions begin to approach the previously unreasonable drag torque limit (drag torque compensation limit). Figure 9 illustrates a simplified block diagram of the RWA manager.

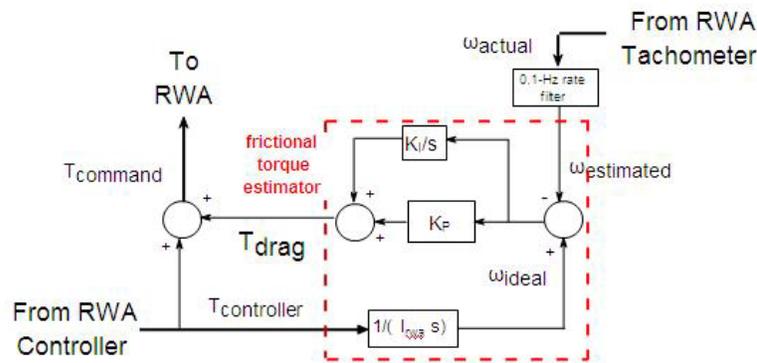


Figure 9. RWA Manager Block Diagram Simplified
RWA Manager block diagram intended to illustrate the drag torque compensation limit parameter.

C. Personnel Changes

Missions with long durations will experience a significant amount of staffing turnover. As a result the FP design needs to be as simple as possible while still being robust to inevitable commanding errors. FP monitors command syntax, enforces command restrictions, maintains attitude constraints, and enforces a number of safe-guards on commands which patch FSW memory addresses. Details about the Cassini FSW patching process are given in reference 1.

D. Mission Event and Mission Goal Changes

Changes in mission events or goals will significantly impact FP. Notably critical sequences, such as SOI, contain significantly different FP logic than nominal mission events. For the SOI burn the FP philosophy was fundamentally different than tour FP since Cassini had a requirement to fail operational instead of fail safe. Other changes such as trajectory impact FP design as well. Trajectory changes to reduce Enceladus flyby altitudes have introduced new FP threats such as control authority and even impact risks. AACS FP design allows operators the flexibility to sensitize or de-sensitize EMs without and code logic changes. Increasing the sensitivities of certain

EMs can reduce the total ΔV imparted in fault conditions which occur before low altitude Enceladus flybys, thereby reducing the risk of impact.

V. Updating FP

As described in Section IV, FP must adapt to new environments and requirements. The Cassini AACS FP is highly parameterized, allowing for modification without changing any check-summed constants. Modification of variables in active RAM FSW, can be performed via memory write commanding and does not require a full FSW load. AACS FP has taken advantage of the high parameterization and has not made any logic changes to the FP design since the SOI FSW load (AACS FSW version A8.7.1). The lack of logic changes in FP FSW has greatly simplified the acceptance testing during subsequent FSW updates. See reference 7 for details about the Cassini FSW testing methodology.

As mentioned in Section III, AACS FP trends FP performance, and evaluates the need to update FP when a threshold is violated or a threatening trend is identified. A worsening trend may be indicative of degrading hardware or FSW model performance. With all FP threshold selection, there is the classic balance between triggering FP too early and creating a false alarm, and triggering too late thereby missing potentially dangerous off-nominal performance. The following few paragraphs address one instance where a new AACS FP parameter was selected.

As described in Section IV, the viscous friction of the RWAs increases slowly with time, threatening the FP threshold for acceptable levels of drag torque. If the estimated drag torque exceeds the drag torque compensation limit parameter or if the torque request exceeds the RWA motor torque capability, a RWA rate error will grow due to the insufficient commanded torque. While AACS has no control over the RWA total torque capability, AACS can increase the RWA drag torque compensation limit parameter to ensure that more or all of the total RWA motor torque is used.

New drag torque compensation limits were selected in a similar manner compared to launch FP design. AACS used two approaches to determine the new limits. The first method simply multiplied the highest observed RWA friction by a factor of safety selected before launch by the RWA manufacturer. The second approach used trends of RWA drag torque over several years to determine an expected rate of increase for RWA drag torque. AACS then extrapolated the drag torque trend through the end of prime mission to determine the expected end of mission drag torque. Both methods agreed within 10% of each other with the more conservative value selected for each RWA.

In addition to responding to anomalous trends in FP performance, pro-active changes are also made to FP. Vulnerabilities discovered through testing or changes in environmental, hardware, personnel and mission events require analysis in anticipation of a problem. For example a fault preceding a low altitude Enceladus flyby (such as the 50 km E3 flyby on March 12, 2008) can impart enough un-modeled ΔV to cause a significant impact probability. With respect to the impact risk specifically, changes in FP thresholds or tier counts were considered to reduce the un-modeled ΔV below a threatening level.

VI. FP that is Routinely Managed

While AACS FP supports the majority of operating scenarios, there are a few instances where FP needs to be managed by ground commanding. While undesirable, AACS FP has developed operational “work-arounds” in lieu of FP design changes. FP management is performed by automated ground software or processes which reduces the likelihood of commanding errors. Daily FP commanding is created by GSW tools to clear all HWMs, at the end of telemetry downlink passes. In addition to clearing HWMs, the FP log is also reset so that new entries will be written over the first lines of the log.

During low altitude Titan flybys, Titan’s atmosphere imparts a torque on the spacecraft. The Cassini FSW has no knowledge of the Titan atmospheric torque (or any other external torque) and will misdiagnose this external torque as a thruster leak. To prevent this action, the FP threshold for the leak detection error monitor, Excessive Thruster Commanding (ETC), is de-sensitized 10 hours before and after Titan closest approach (TCA) via commanding. AACS maintains command blocks which are re-used during each Titan flyby to prevent any commanding error while modifying the ETC monitor’s parameters.

Cassini employs a Constraint Avoidance in Progress (CAIP) EM to enforce geometric and dynamic constraints. If triggered, the response to the CAIP EM is to request system Safing. When the CAIP EM is masked a local response is triggered despite the EM outputting no opinion. This local response will enforce the constraint, causing either a truncation of the rate/acceleration or an attitude deviation which “walks around” the geometric violation, minimizing the difference between commanded attitude while enforcing the geometric constraint.

The Safing response for CAIP is too unforgiving for most operating scenarios and so the EM is nominally masked, allowing the local response to take graceful action to avoid the constraint without invoking Safing. The one instance where the CAIP error monitor is unmasked is during maneuvers where it is unacceptable to deviate from the commanded attitude and potentially burn in the incorrect direction. During maneuvers ground software (GSW) tools are employed to autonomously build all of the required maneuver commands which includes the management of the CAIP EM. A detailed description of the Cassini maneuver process is provided in reference 8 which describes how Cassini has executed over one hundred maneuvers in tour without error.

AACS FSW has the capability to suspend star identification (SID) during times of predicted SID outages when to bright bodies enters the SRU field of view (FOV). This capability has proven to be extremely important during tour operations with SID being suspended hundreds of times for Saturn, the rings, Titan, Enceladus and many other bright moons. During SID suspends no inertial attitude star updates take place. This threatens an EM which checks for the regular occurrence of star updates. Due to this vulnerability this EM is masked during periods of time where SID is suspended. A ground software tool checks for the need to issue SID suspends and autonomously builds the necessary SID suspend command along with the EM masking and unmasking commands. It is worth noting that the lack of requirements to perform SID while small bright bodies are in the SRU FOV during the time of hardware selection required a FSW work-around to perform SID suspends. This is an example of how FP decisions and solutions can be implemented at the hardware level.

VII. Conclusions and Lessons Learned

Several factors combine to allow AACS FP to successfully support Cassini operations for over 10 years, robust yet adaptable design, proactive FP monitoring and planning, and limited FP logic changes. The Cassini AACS FP design was an enormous effort by a number of engineers who have preceded the author of this paper, and the effectiveness of the AACS FP is a testament to their tireless effort.

Throughout Cassini's prime mission, there have been several lessons learned. FP complexity is a major topic that requires discussion. The spacecraft attitude control algorithms are complex, which necessitates complex monitors to evaluate their performance. With increased FP complexity, FP updates and validation become challenging. Timing jitter and unintended interactions become more difficult to identify and test. Cassini AACS FP and System FP (SFP) can both detect and respond to anomalous behavior. Careful coordination between AACS FP and SFP thresholds and persistence limits is critical to ensure no undesirable interactions between Cassini FP. Response scripts use state information provided by repair managers, the mode commander, configuration manager and hardware interface managers to determine an appropriate action. While AACS FP is internally quite robust, actions from outside AACS FP which can affect the S/C state without informing AACS FP can lead to undesirable interactions. Care needs to be taken during the design phase to ensure that all state assumptions made by AACS FP are valid, and that all commands issued outside of AACS FP which can impact AACS state need to be considered.

A major strength of the FP architecture is the state-space based error test that Cassini utilizes in many of the control and estimation EMs. This greatly increased FP resiliency to transient anomalous behavior. Events such as the first star update following a period of suspended SID, updates to the Cassini vector, or rate spikes due to a high energy proton striking a gyro can all create an attitude discontinuity that would otherwise threaten FP EMs. In this way FP can avoid a hair trigger response while still responding quickly to truly dangerous anomalous behavior.

A lesson learned from many missions is to incorporate FP engineers as early in the design cycle as possible. Sometimes seemingly logical assumptions can cause problems in anomalous conditions. For example, the RWA tachometer does not take wheel speed measurements when the RWAs are unpowered. In fault scenarios when the RWAs are powered off the FSW wheel speeds remain "frozen" at the last tachometer measurement. As friction brings the wheel speeds to zero a mismatch grows between the FSW wheel momentum and the physical wheel momentum. This momentum mismatch can cause the ETC error monitor to incorrectly diagnose a thruster leak for which the response results in unnecessary hardware swapping.

Another benefit of considering FP early in the design cycle is to incorporate FP design into the hardware. One example of FP design which manifests in hardware are SSPS which power AACS equipment. Power is supplied to the AFCs by two SSPS which share the current load evenly. In the event of an SET-induced SSPS trip, a single line SSPS enters a high impedance state leaving the other SSPS to carry the entire current load. The SSPSs for the AFCs are sized for this and the result is no loss in power for the AFC. No FP design in FSW will be able to recover from this fault without the loss of power to the AFC with a single line SSPS.

As a general rule, it is highly encouraged to keep FP algorithms and design as simple as possible while achieving still FP goals. Additional low level error monitors which can directly monitor a particular hardware performance

metric would allow FP to detect and respond to a specific fault more quickly but increase the overall FP complexity. Despite the large number of hardware interface EMs, Cassini FP still relies heavily on control and estimation error monitors to catch any faults which may not be caught by low level fault protection. In this way is unclear that additional low level monitors in Cassini AACS FP would increase the fault coverage, and only increase FP complexity.

While missions benefit from keeping the FP design as simple as possible, increasing visibility into FP actions is greatly beneficial. FP activity logs and FP telemetry are essential for ground operators to diagnose complex faults and determine FP actions. While FP logs are easy to store and recover following FP activity, the bandwidth for FP telemetry is often limited. Care needs to be taken to ensure that FP telemetry resolution isn't so coarse that it is rendered useless. The Cassini AACS uses several telemetry schedules each containing various telemetry channels at different frequencies. During major anomalies FSW will select a different telemetry schedule which contains higher frequencies of FP-centric telemetry. Unfortunately the telemetry that is often of greatest interest is the time before the anomalous behavior and it is unavailable, or infrequent. In cases such as this FP engineers may need to rely on FSW testbeds to recreate a fault event. Refer to references 2 and 7 for more information about testing and the Cassini Flight Software Development System test platform.

While remaining versatile, FP needs to be easy to modify to be robust to changes in environment and hardware performance. Cassini FP has benefited from being highly parameterized, allowing for easy modification and tuning without any FP logic changes. Thresholds and persistence limits have been modified several times during Tour operations to better tune AACS FP for the environment and the changing hardware performance. Avoiding logic changes to FSW greatly simplifies testing, and operations team workload. In addition to tuning FP EMs, AACS can also affect FP via commanding. AACS has a number of commands to mask, unmask, desensitize EMs, clear HWMs, reset FP logs, block or un-block mode transitions, modify FP visibility through telemetry schedules, direct FSW variable readouts, forced telemetry packet output, and alter the hardware health by marking specific hardware sick, dead or failed. These commands greatly increase the ground operator's ability to affect FP without FSW logic changes.

While FP is intended to support all operating scenarios, there are occasions where this is not possible, as mentioned in Section VI. If ground commanding is required for certain predictive events, Cassini GSW tools can generate the necessary commands autonomously. This greatly reduces the operational load and increases mission reliability by removing some of the "human error" factor. A major contributing factor which reduced operator error over Cassini's lengthy prime mission is the high level of autonomy of GSW monitoring tools, sequence and maneuver generation and development.

For long missions that expect to experience hardware and algorithm degradation, trending EM performance is an important activity. Trending FP performance can be a highly automated process, requiring little effort. Proactively monitoring FP trends and preemptively making the necessary parameter or FP updates can help eliminate some of the reactive time pressured FP design or FSW updates.

The Cassini operations team has seen turnover in personnel during the lengthy design phase and prime mission. Training material and documentation have been crucial resources for new engineers. A training pipeline is essential for long missions where high employee turnover is expected. Due to FP complexity, the FP engineers can sometimes become a single-point-failure themselves! The Cassini FP Design Document (FPDD) includes a detailed description of all EMs, response scripts, activation rules, repair managers, and redundancy managers employed by Cassini AACS FP. The FPDD includes the rationale for each error monitor and the rationale for the threshold and persistence selection. This kind of resource is extremely useful when FP engineers decide to update FP limits.

Although the Cassini AACS FP design is complex, it has been very robust during Cassini's prime mission. Despite the turnover in operations team personnel, cooperate knowledge remains through detailed documentation, such as the FPDD, as well as training exercises. Careful AACS FP design resulted in highly parametric FP algorithms and EMs allowing for large flexibility without logic changes. Early inclusion of FP considerations in the AACS design process led to the robust design and the inclusion of FP design in the hardware and software architecture which would have otherwise not been possible.

Acknowledgments

The work described in this paper was carried out by Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The Cassini AACS FP design was an enormous effort made by a number of engineers who have preceded me, and the effectiveness of the Cassini AACS FP is a testament to their tireless efforts. Current and previous engineers who have greatly impacted

the Cassini AACS FP design include: Jim Alexander, Kevin Barltrop, Douglas Bernard, Jay Brown, Mark Brown, Tom Burk, Larry Chang, Paul Enright, Ken Friberg, Gene Hanover, Juan Hernandez, Katie Hilbert, Sue Johnson, Allan Lee, Danny Lam, Glenn Macala, Scott Peer, Robert Rasmussen, Sam Sarani, Guru Singh, Eric Wang and Julie Wertz.

References

¹Brown, J. M., "Cassini Attitude Control Flight Software: From Development to In-flight Operation," *AIAA Guidance, Navigation, and Control Conference and Exhibit*, Honolulu, HI, Aug. 18-21, 2008.

²Brown, J. M., Lam, D.C., Chang, L., Burk, T.A., and Wette, M.R., "The Role of the Flight Software Development System Simulator throughout the Cassini Mission," *AIAA Guidance, Navigation, and Control Conference and Exhibit*, AIAA-2005-6389, San Francisco, CA, Aug. 15-18, 2005.

³Brown, M. B., Johnson, S.A., "An Overview of the Fault Protection Design for the Attitude Control Subsystem of the Cassini Spacecraft," *American Control Conference*, Philadelphia, PA, June 1998.

⁴Carr, G., and Ging, A. T., "The Cassini Power System Performance over the Last Decade", *5th International Energy Conversion Engineering Conference and Exhibit*, St. Louis, Missouri, June 25-27, 2007.

⁵Lee, A. Y., and Hanover, G., "Cassini Spacecraft Attitude Control System Flight Performance," *Proceedings of the AIAA Guidance, Navigation, and Control Conference, and Exhibit*, San Francisco, California, August 15-18, 2005.

⁶Macala, G. A., "A State-Space Fault Monitor Architecture and its Application to the Cassini Spacecraft," *American Control Conference*, Philadelphia, PA, June 1998.

⁷Wang, E.K., and Brown, J.M., "Cassini Test Methodology for Flight Software Verification during Operations," *15th AIAA Guidance, Navigation and Control Conference and Exhibit*, Hilton Head, SC, Aug. 20-23, 2007.

⁸Yang, G. V., Mohr, D., and Kirby, C., "Cassini's Maneuver Automation Software (MAS) Process: How to Successfully Command 200 Navigation Maneuvers Without Failure," *AIAA Guidance, Navigation, and Control Conference and Exhibit*, Honolulu, HI, Aug. 18-21, 2008.