

# **Fault Protection Design and Testing For the Cassini Spacecraft in a “Mixed” Thruster Configuration**

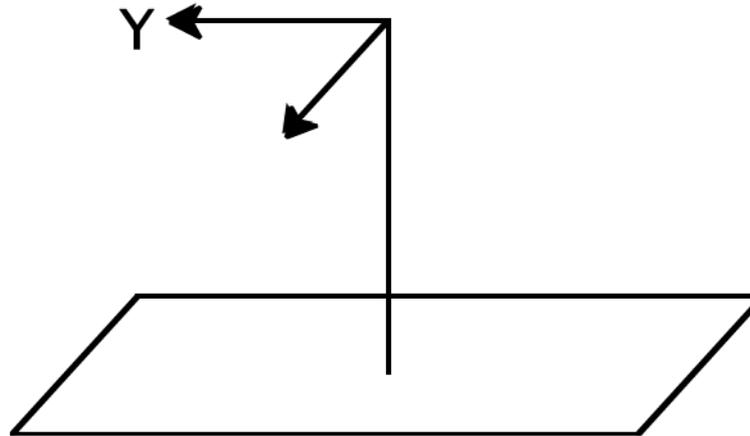
**August 19, 2013**

**David Bates**

**Jet Propulsion Laboratory,  
California Institute of Technology**

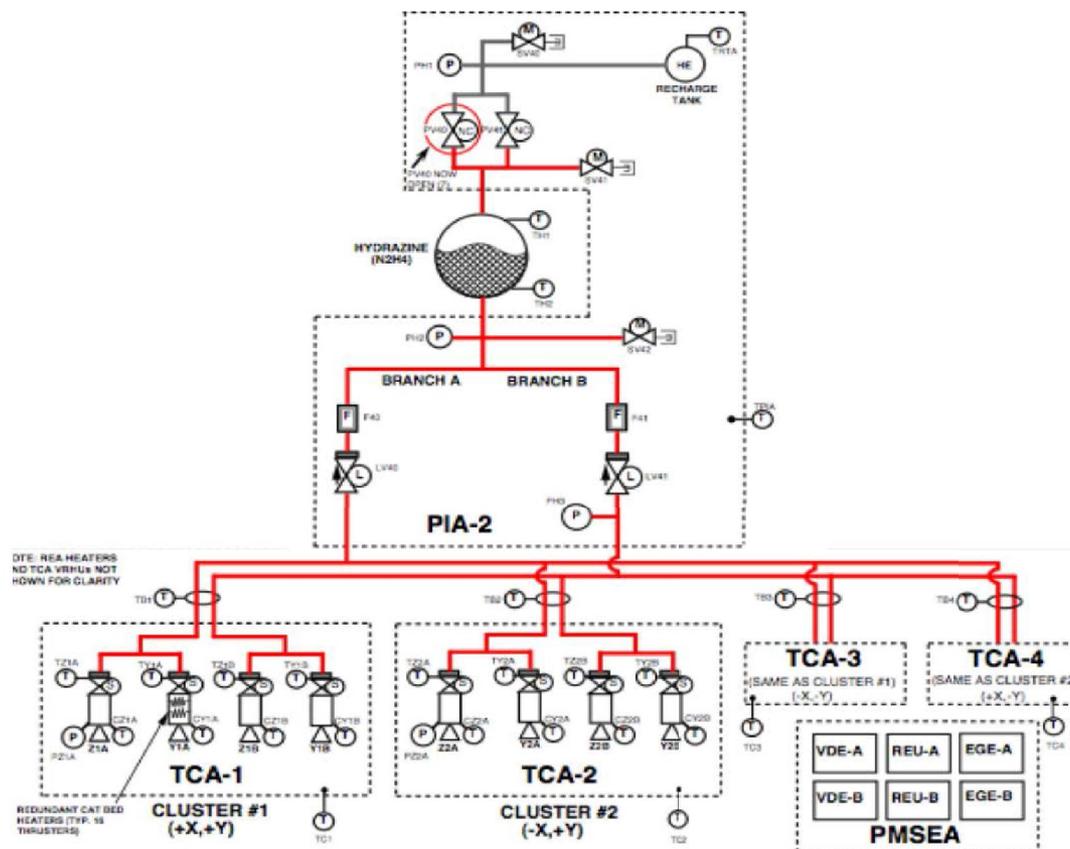
# Cassini Reaction Control System Background

- Cassini has two independent branches of monopropellant hydrazine Reaction Control System (RCS) Thrusters
  - Prime and Offline Backup, essentially collocated
  - Used for 3 axis control and translation velocity changes



# Cassini Reaction Control System History

- In October of 2008, swapped to B-branch thrusters because of degradation in two of the A-branch thrusters
- Corresponding Latch Valves, catbed heaters, and driver electronics all swapped to B-branch



## Problem With AACCS Fault Protection in “Mixed Mode”

- If B-branch thrusters degrade, may need to go to mixed branch mode
  - Use some A-branch thrusters with some from B-branch
  - Cassini attitude control flight software is capable of supporting mixed branch configuration
    - Ground operators designate which set of thrusters, catbed heaters, and driver electronics on the two branches are prime
- The original FP logic did not handle mixed branch thoroughly

# Problem With AACCS Fault Protection in “Mixed Mode”

- Cassini FP includes thruster leak detection error monitors which use the Euler equations to monitor for excessive thruster commanding (ETC).
  - Compares expected angular momentum accumulation with estimates of commanded RCS and Reaction Wheel Assembly (RWA) control quantities.
  - Response to ETC error is a number of corrective actions that swap hardware and call safing
    - Based on tier count that increments each time ETC is detected
    - On the sixth tier count, swap to backup thruster branch and close appropriate latch valve
      - Does not swap thruster branches a second time
      - Does not stop backup thruster branch leak
  - Original design was single fault tolerant

# Design of Mixed Branch Fault Protection

- Three main design options considered to protect against leaking thruster in mixed branch configuration



- Design FP to close both upstream latch valves and transition to RWA based safe mode
  - Mitigates widest variety of thruster failures
  - Requires large design changes and testing
    - » Detumble, sun search, find stars, turn to safe attitude was designed and thoroughly tested using RCS control



- Design FP to diagnose which thruster is leaking, and swap to opposite branch
  - Allows for RCS safing recovery
  - Requires complex logical additions to the code



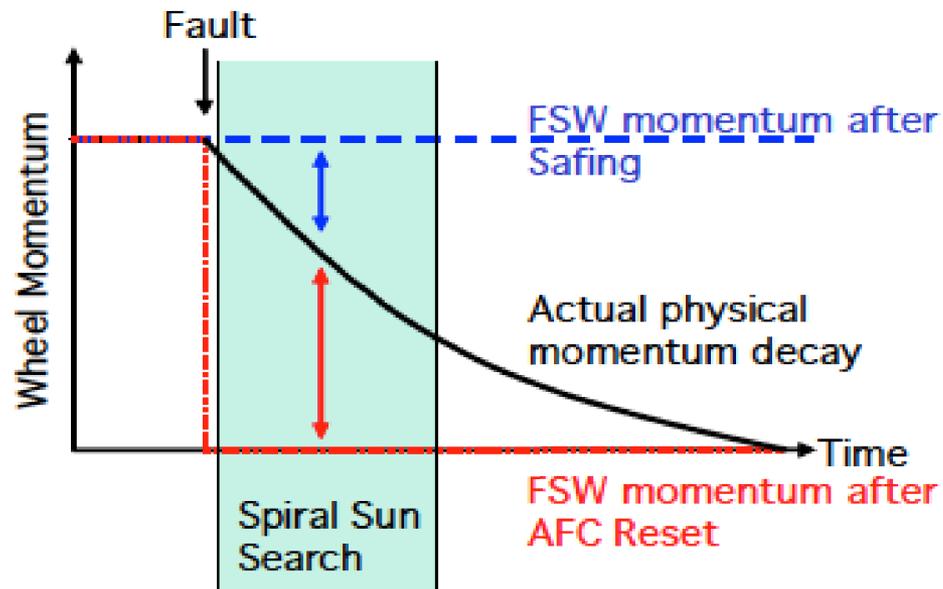
- Design FP to swap thruster branches twice, if needed
  - Simplest option to code and test
  - Uses more hydrazine before leak is mitigated

# Mixed Branch RCS Fault Protection Testing

- Extensive amount of testing on multiple platforms performed for every update to the Attitude and Articulation Control Subsystem Flight Software
  - Verify proper design and implementation of the update under multiple configurations and scenarios
  - New test cases designed to target the mixed branch FP changes
    - A or B-branch RCS thrusters stuck open or closed
    - Latch valve and drive electronics failures
    - RWA faults
    - Attitude determination functional failures
    - Etc

## Interesting Test Results

- Test results showed successful mixed branch fault protection design and implementation
- A few extreme scenarios revealed unexpected results
  - Phantom momentum induces false ETC fault trip
    - A known mismatch between the FSW modeled RWA momentum and the actual momentum can occur when the RWA system is unexpectedly powered off



# Interesting Test Results

- A few extreme scenarios revealed unexpected results
  - Interfering Fault Responses
    - Object oriented FP design allows multiple response scripts to be active at same time
    - In a few test cases involving stuck closed thrusters, the excessive attitude error monitor interfered with the ETC tier count, so the thruster swap occurred later than expected
      - » Both monitors were overwriting the tier counter
      - » Requires extensive code changes to fix
      - » Stuck close thrusters don't leak hydrazine, so risk deemed acceptable
  - Safety Net Fault Responses
    - Routines that react when lower level fault protection is unable to mitigate faults
    - Excessive hardware swapping occurs prior to fault mitigation
    - Handful of test cases had extraneous hardware swaps, but fault was eventually mitigated

# Conclusion

- Successful design, implementation and testing of the update to Cassini mixed RCS branch AACS Fault Protection Flight Software was a huge team success
- Lessons learned
  - Design software to fully make use of hardware redundancy
    - FSW handled mixed branch in nominal operations, not in fault scenarios
  - Maintain strict adherence to object-oriented paradigm
    - Phantom momentum
      - » One FSW object powered off reaction wheels without telling other objects
    - Fault monitor counter interference
      - » Two fault monitor objects overwrote the same counter
  - Test environments should have scripting capability
    - Test cases can be easily modified, evaluated, re-run, and compared against previous versions of FSW