

Flip-A-Bit

Dawn's Fault Protection System & Lessons Learned

Dave Termohlen – Dawn Software Lead
termohlen.david@orbital.com

Dawn

- ◆ Objective: To orbit Vesta & Ceres, two of the largest asteroids in the solar system, in a quest to understand the conditions and processes during the earliest history of our solar system
 - Vesta – Volcanic
 - Ceres (now categorized a mini-planet) – 25 miles of ice
- ◆ Eight to ten months of observations at each asteroid
- ◆ Dawn uses Solar-Electric-Propulsion (Ion Engines)

Dawn

◆ Instruments:

- Framing Camera (DLR)
- Mapping Spectrometer (ASI)
- Gamma Ray & Neutron Detector (LANL)
- Gravity Science (JPL)

Fault Protection

- ◆ What is a fault?
 - Single-event (soft) upset (Flip-A-Bit)
 - Sensor or actuator fault
 - Hardware fault
 - Operator?
- ◆ How many simultaneous faults are tolerable?
- ◆ How are faults sensed and corrected?
- ◆ How fast do we need to respond?

Dawn's Baseline

- ◆ Dawn's original design was based on SORCE (a simple Low-Earth-Orbiting spacecraft)
 - The design included a safehold processor
 - Many faults lead to safehold
 - Safehold points the solar arrays at the Sun and maintains the spacecraft in a low-power state

Single-Fault-Tolerance

- ◆ Single Fault Tolerant means that the spacecraft can endure any single fault without impact to the mission
- ◆ Orbital had considered transition to safehold a fault... JPL does not consider operator error as a fault
- ◆ Safehold was eliminated in favor of ARM (Autonomous Redundancy Management)

Autonomous Redundancy Management (ARM)

- ◆ ARM is managed through the cooperation of two “watchers” and the On-Board-Computer (OBC)
- ◆ The “watcher” function was implemented in the (cross-linked) uplink cards



Telemetry Monitors

- ◆ Telemetry monitors perform range checks on telemetry with a persistence setting
- ◆ Response is a telemetry bit indicating that a condition is met
- ◆ Response may also include the initiation of a Relative Time Sequence (RTS)

Telemetry Monitors

- ◆ Each telemetry monitor may have four-tiers of evaluation
- ◆ Complex monitors may be supplemented by C-code “derived functions”
- ◆ Telemetry monitors can be cascaded to evaluate telemetry from multiple packets

Design Evolution

- ◆ For LEO spacecraft, faults are typically handled at a very high-level
 - Battery depth-of-discharge
 - Excessive rate
 - Inability to command the reaction wheels
 - Loss of 1553 traffic

Design Evolution

- ◆ Dawn is considered "Semi-Robotic"
 - Spacecraft must be able to remain safe for one week without ground intervention
 - Power-positive
 - Reaction Control System and Ion propulsion must be maintained (isolation of leaks)
 - Thermal control of critical subsystems

Design Evolution

- ◆ Telemetry monitors needed to be doubled from 128 to 256
- ◆ RTS' needed to be doubled from 128 to 256
- ◆ Ported telemetry monitors, RTS', and SM task (needed for table maintenance) to Uplink card
- ◆ Implemented a *masked* disable for TMON system

What Made The Job Tough

- ◆ Design was a collaboration between JPL and Orbital
- ◆ Fault Protection was originally estimated to be a six man-month effort... turned into a six man-year effort
- ◆ The number of sensors (primarily thermal) more than doubled from the baseline

What Made The Job Tough

- ◆ Failure modes analysis was not performed early enough or at a sufficiently detailed level
 - Resulted in a design that was driven by possibility of fault... not probability of fault
 - Resulted in three-fault-deep TMON's

What Made The Job Tough

- ◆ Fine-grained
 - The heritage Telemetry Monitor design only evaluates a single value from a single telemetry packet
 - Many TMON's were needed to evaluate a single condition
- ◆ Disconnected response
 - Multiple RTS' could have conflicting actions

Looking Forward

- ◆ Need a way to evaluate a condition with a single equation
 - Multiple telemetry points (channels) evaluated in a single pass
 - Need ability to identify stale or zero'd (initial conditions) telemetry
 - Requires additional CPU bandwidth

Looking Forward

- ◆ Need a way to synchronize and/or prioritize responses (RTS')
 - Baseline design assumed only single response running at one time
 - Heritage RTS' system limits number of commands issued in one second to 14 (aggregate of all RTS')

What Are Your Questions?

A satellite is shown in space, oriented diagonally. It has two long solar panel arrays extending from a central body. One array is on the left, and the other is on the right. The central body features a large, white, circular dish antenna. The background is a dark, reddish-brown planet with a smaller, grey, spherical moon in the upper right. The overall scene is set in a dark, starry space.

11/5/2007