Effective CubeSat Fault Management Strategies Beyond Low Earth Orbit

Interplanetary Small Satellite Conference

May 1-2, 2017

Matt Sorgenfrei, PhD
Intelligent Systems Division
NASA Ames Research Center

Outline

- BioSentinel Mission Overview
- Fault Management Approach
- Propulsion Fault Management Example
- Future Work

The BioSentinel Mission

BioSentinel: A Deep Space CubeSat

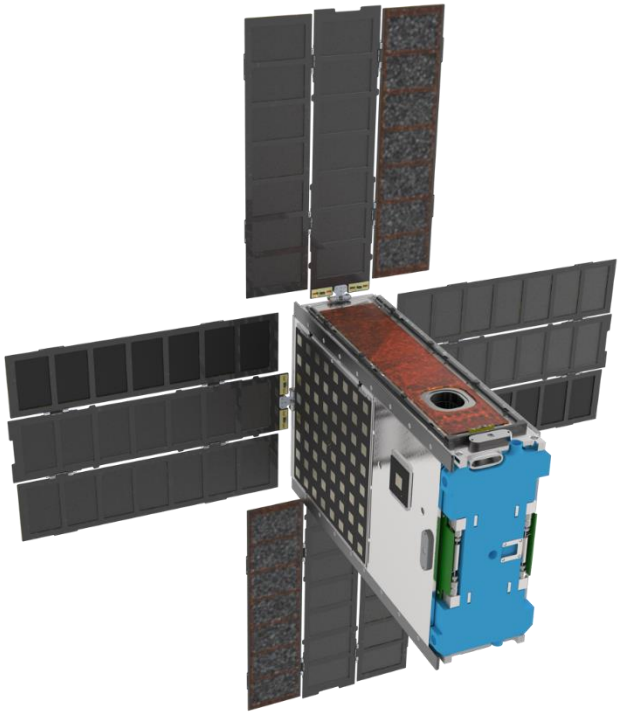


Figure 1. The BioSentinel spacecraft, shown with solar panels deployed

- A 6U CubeSat that will launch on the first flight of the Space Launch System (EM-1)
- Will operate in an Earth-trailing, heliocentric orbit
- Requires active attitude determination and control and a propulsion system to support nominal operations
- Science payload will study the effects of deep space radiation on a colony of yeast cells (eukaryotic—good analogy for humans)

Valuable Access to Deep Space

- BioSentinel will characterize radiation environment for future human exploration of deep space
- Deduced by observing behavior of yeast cells in the presence of high-energy particle strikes
- Launch on EM-1 provides access to environment beyond the Earth's magnetosphere
- Linear Energy Transfer (LET) sensor will provide complementary radiation data

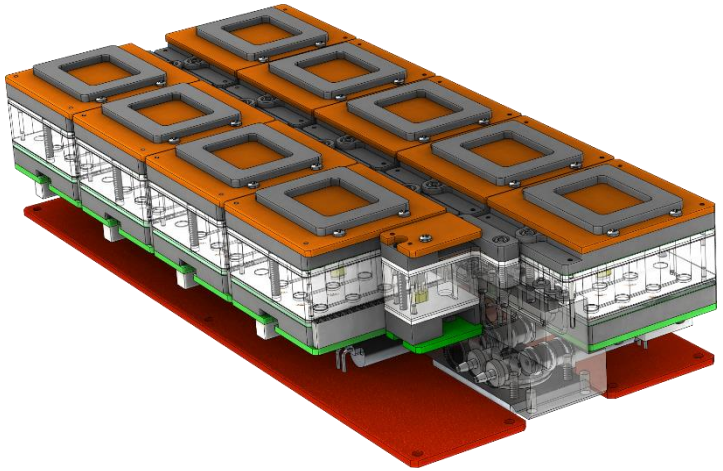


Figure 2. One half of the BioSensor payload, which will study the impact of radiation on DNA.

Fault Management Considerations

- Thermal sensitivity of biology payload is of greatest concern when ensuring top-level mission success
- BioSentinel will have at most 3 communications passes of roughly 30 minutes with the Deep Space Network per day
- Data rates are such that very few faults will be actionable from the ground (and never in real-time)
- Fault management software must be able to detect off-nominal behaviors and intercede without direction interaction with Mission Operations System (MOS)

Fault Management Approach

Mission Phases and Mode Transitions

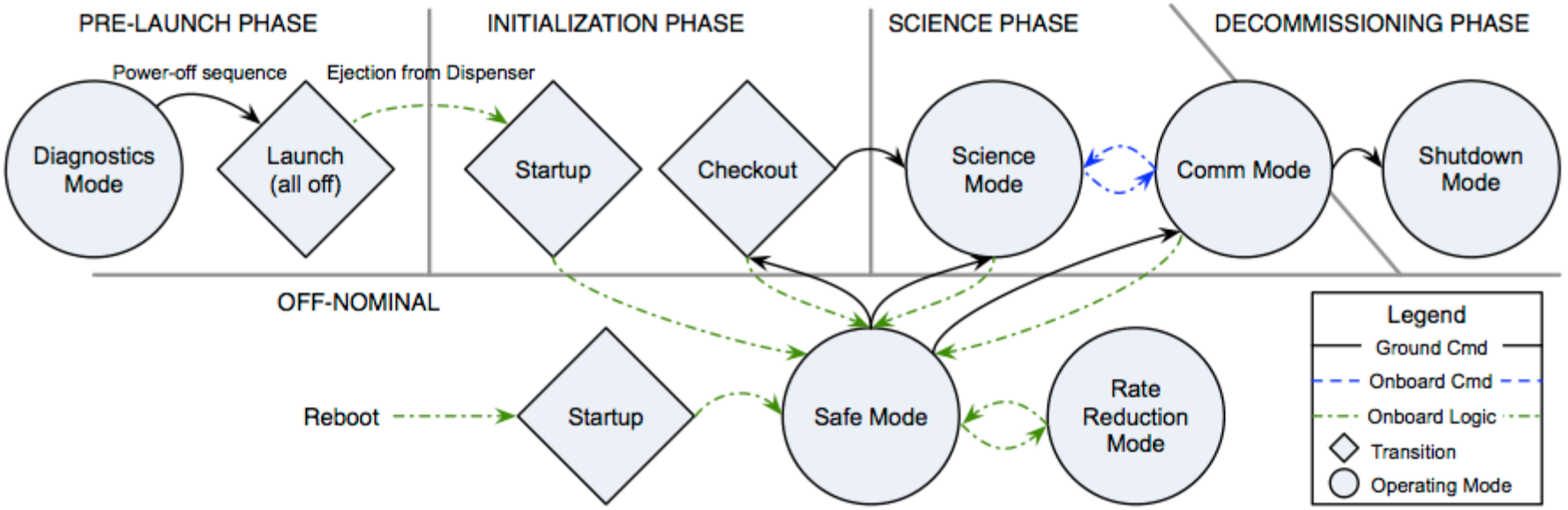


Figure 3. Spacecraft operating modes and their allowed transitions over all phases of the BioSentinel Mission

Possible On-Board Responses

- No response
  - Failure modes for which no response will be taken are tracked as risks at the Project level
- Record telemetry for MOS
  - Managed through strike counters and event messages
- Flight software action
  - Limit checkers, memory scrubs, etc.
- Flight hardware action
  - Autonomous hardware actions, such as entering into Safe Mode

Watch Points/Action Points Detail

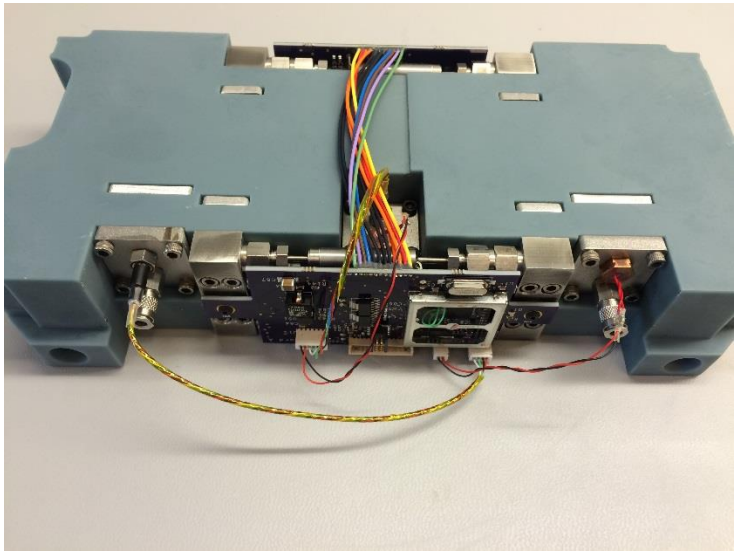
- Each subsystem identifies telemetry points that should be monitored by the limit checker
- Unique watch points (i.e. reaction wheel rate limit) are assigned specific strike counts that are also monitored by the limit checker
- When a specific watch point exceeds its strike count it can trigger an action point (such as transitioning to safe mode)
  - Those action points can be reset autonomously or manually via MOS
- Multiple telemetry points can be combined into a specific watch point, depending on the needs of the subsystem

Additional Flight Software Actions

- Strike counters associated with all subsystem telemetry watch points will be recorded and sent to MOS as part of standard telemetry
- Event messages can be generated by flight software at higher frequency than standard telemetry
  - Specific event messages will be designed for specific fault scenarios
- Flight software limit checker will constantly monitor all watch points, and if necessary an associated action point will trigger a relative time sequence (RTS) script
- Due to communications challenges resulting from deep space operations limit checker is first/best line of defense

Fault Management Example

Propulsion System Thermal Limit (1/2)



- The cold gas propulsion system being used for BioSentinel has a nominal upper-bound on operating temperature of 50 °C
- Temperature and pressure sensors are located inside both the main tank and the expansion tank
- Watch point/actions points are designed to ignore individual out-of-bounds measurements, while protecting against an overheating condition

Propulsion System Thermal Limit (2/2)

- Watch point: All propulsion system temperatures and pressures
- Action point: If any individual sensor is out of range 10 times in a row (10 seconds), reboot the propulsion system
- Watch point: Main tank pressure AND main tank temperature
- Action point: If both main tank pressure and main tank temperature are out of range 12 times in a row, vent the plenum to reduce pressure in the main tank

Future Work

- Further development of the watch points and action points for all subsystems
- Refinement of downlink budgets for each subsystem for commissioning and nominal operating phases
- Continued development/testing of limit checker autonomy
- Even more testing

Questions?

matthew.c.sorgenfrei@nasa.gov