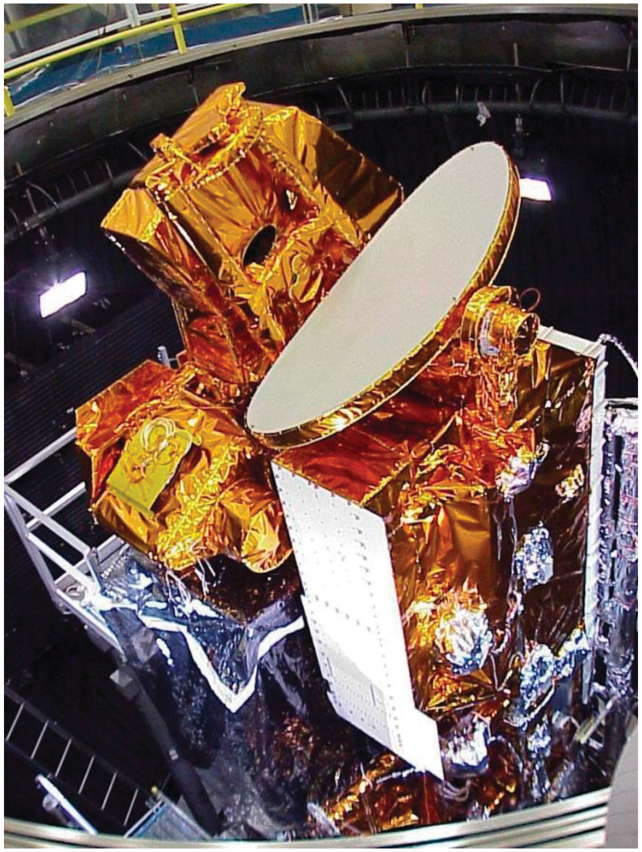

EOS MLS Lessons Learned

Design Ideas for Safer & Lower Cost Operations

Dominick Miller

Jet Propulsion Laboratory

California Institute of Technology

A Little History

- The Earth Observing System (EOS) Microwave Limb Sounder (MLS) is a complex instrument with a front end computer and 32 subsystem computers
- MLS is one of four instruments on NASA's EOS Aura spacecraft
- With almost 8 years in orbit, MLS has a few lessons learned which can be applied during the design phase of future instruments to effect better longevity, more robust operations and a significant cost benefit during operations phase
- While some items may seem obvious, their continued persistence suggests that they are worth mentioning

Operational Concepts

Autonomous Operations

- In comparison with other instruments, MLS enjoys a significant benefit because nominal operations are largely autonomous
- By design, MLS requires no commands for nominal science; the instrument operates 24/7 once initialized

The message

- Designing instruments with autonomous operations (as much as possible) has significant science and cost benefits in the operations phase

Instrument Safing and Fault Responses

In the beginning…

- MLS safing and fault responses tended to be cautious with safe mode considered as a “catch all” kind of response

As the world turned and the spacecraft aged…

- All four instrument teams quickly became concerned about thermal impacts when an Aura spacecraft fault may have required that the instruments be transitioned to Safe mode

The message

- Initial safing and fault management responses should also consider the impacts of thermal cycling
- Respond to the issue, but don’t over-respond

Flight Software Design

It’s been said that, if the flight software (FSW) person had to operate the instrument, they would likely code the software differently

- While the software may meet requirements and function perfectly, it can still be difficult operationally

The message

- Connect the FSW designer with an operations person early in the process so that the FSW architecture does not become cumbersome to operate

The following few slides illustrate a few examples of where early intervention could have benefitted the MLS FSW

A Few MLS FSW Examples

Configurability

- MLS instrument configuration is accomplished via a table upload which contains all subsystems
- While reasonable on some levels, this approach makes fault management responses much more complicated as the full table must be generated to shut down a single subsystem
- The logic required to generate this table is complex

The message

- FSW should allow for single subsystem reconfigurations without addressing all subsystems

A Few MLS FSW Examples

Diagnostics

- When an MLS subsystem is shut down by onboard Fault Management (FM), there is no telemetry stored which identifies the cause of the shutdown
- During some reconfigurations, the MLS FSW must be placed in a mode that masks errors

The message

- Store an error code, send a letter, write home to Mom… preserve some level of “core dump” information in non-volatile memory when things go astray

A Few MLS FSW Examples

Fault Management

- MLS commanding is largely done on real time 20 minute contacts with the spacecraft
- As currently implemented, disabling and re-enabling Fault Management (FM) consumes 30 to 60% of the contact time
- A better implementation of FM is seen at the Aura spacecraft level where there are separate controls for limit checking and responding

The message

- While critically important, FM should also be tolerant of transitional periods

MLS FSW Issues

Three unrelated features

1) The software counter

- After launch it was found that an MLS software counter was missing a single increment 70% of the time a specific command was used
- Of course it would have to be our most frequently used command but, it’s only used during reconfigurations and has no impact on science data; so why should it matter?

MLS FSW Issues

Three unrelated features

2) The mechanism start command

- MLS uses 3 mechanisms to scan the atmosphere
- During ground testing for a special extended scan activity, it was accidentally discovered that MLS mechanisms would go anomalous if they received a second start command while executing a scan
- But why would we ever send a second start command in the middle of a scan?

MLS FSW Issues

Three unrelated features

3) The fault management

- MLS FM was tested during Integration and Test (I&T)
  - If a subsystem faulted, it would get powered down by the fault management software
  - If a second subsystem faulted, it too would get powered down
- Unfortunately, once in orbit it was found that, if two subsystems faulted at the same time, the FM software would get fooled into thinking that many of the 32 subsystems had faulted and shut them all down
- But how likely is it that multiple subsystems would fault at the same time?

The MLS Grand Finale

A triple fault with a ½ to ¾ twist

1) If (and only if) the software counter skips at precisely the wrong count

2) Active mechanisms receive a second start command causing them to simultaneously go anomalous

3) Thereby activating the multiple fault "feature" of the FM software

- Which then shuts down ½ to ¾ of the instrument

… Murphy is a perfectionist

Interdependent Faults

- In retrospect, it appears that these very anomalies may have been seen during I&T but they were infrequent and “passed off” as glitches

The messages

- As the complexity of a system increases the likelihood of interdependent faults increases more than one might expect The K.I.S.S. principle applies

- As much as I&T is a very busy and expensive time in the project timeline, it is still less costly to find hidden bugs during I&T when compared to finding them in a post launch environment

Testbeds

Some projects have forgone the idea of having a testbed as a cost saving measure

- While this may save money up front, it is highly likely to cost many times the price of a testbed in lost science and work hours when trying to analyze new-found features in orbit
- The previously mentioned MLS features would have been nearly impossible to decipher without a testbed

The message

- The value of a testbed with a reasonable level of fidelity can not be overstated

Other Tidbits….

- During a major recovery activity, two real time command counters were reporting 3 extra commands causing concerns of a much bigger problem
  - By the following contact, the command counters had reverted to the expected values
- Subsequent investigations of both instrument and ground system data records did not support the anomalous counts observations

The message

- Two sets of eyes during real time commanding are worth their weight in sanity
  - This ground system anomaly is still under investigation

Summary

- Fly as you test, test as you fly is the motto here at JPL but, at some point, you have to launch and additional “features” will be found
  - On EOS MLS, we’ve been fortunate that none of these new features have been life threatening and we now have work arounds for all of them

- Acting on these lessons learned during the initial design phase can prevent some of the issues presented here and can have very significant benefits in science data, cost savings and instrument longevity during Phase E

Operations Design Take Aways

- Autonomous operation as much as possible
- Operators involved in early FSW architecture
  – Easily configurable subsystems
  – Fault management tolerant of transitions
  – Preserve core dump diagnostics
- Fault responses should also be thermally friendly
  – Respond to the issue, but don’t over-respond
- Significant effort to understand I&T “glitches”
  – Parallel path if necessary
- Interdependent faults; K.I.S.S where possible
- Testbed with reasonable fidelity is critical