

LADEE Preparations for Contingency Operations for the Lunar Orbit Insertion Maneuver

Howard Cannon
NASA Ames Research Center
MS 269-1
Moffett Field, CA 94035
650-604-4606
Howard.N.Cannon@.nasa.gov

Peter Berg
Stinger Ghaffarian Technologies
NASA Ames Research Center
MS 269-3
Moffett Field, CA 94035
650-604-1083
Peter.Berg@.nasa.gov

Anupa Bajwa
NASA Ames Research Center
MS 269-4
Moffett Field, CA 94035
650-604-1851
Anupa.R.Bajwa@.nasa.gov

Alan Crocker
NASA Ames Research Center
MS 241-20
Moffett Field, CA 94035
650-604-1698
Alan.R.Crocker@.nasa.gov

Abstract— The Lunar Atmosphere and Dust Environment Explorer (LADEE) spacecraft was launched on September 7, 2013 UTC, and completed its mission on April 17, 2014 UTC with a directed impact to the Lunar Surface. Its primary goals were to examine the lunar atmosphere, measure lunar dust, and to demonstrate high rate laser communications. The LADEE mission was a resounding success, achieving all mission objectives, much of which can be attributed to careful planning and preparation. This paper discusses the specific preparations for fault conditions that could occur during a highly-critical phase of the mission, the Lunar Orbit Insertion (LOI).

TABLE OF CONTENTS

1. INTRODUCTION	1
2. ONBOARD FAULT MANAGEMENT DESIGN	2
3. DESIGN OF LOI CONTINGENCY OPERATIONS	3
4. CONTINGENCY PROCEDURES PREPARATION	6
5. MISSION OPERATIONS STAFFING	7
6. TESTING AND TRAINING	7
7. OUTCOME AND CONCLUSION	7
ACKNOWLEDGMENTS	8
REFERENCES	8
BIOGRAPHY	9
APPENDIX A: ACRONYMS	9

1. INTRODUCTION

The Lunar Atmosphere and Dust Environment Explorer (LADEE) mission objectives were to examine the structure and composition of the tenuous atmosphere of the Moon and to understand its dust distribution. In addition to carrying payload instruments to achieve these science goals, LADEE provided a platform for a technology demonstration of two-way laser-based communications from lunar distance. [1]

The LADEE spacecraft was a Small Orbiter, Category II Enhanced-Class D spacecraft built upon a modular common bus architecture as shown in Figure 1. [2] LADEE's onboard Guidance, Navigation, and Control (GNC) subsystem design included various control modes (such as Delta-V, Safe Mode, Fine Pointing Mode) to orient the spacecraft for maneuvers, communications, and science. The GNC system determined spacecraft attitude using inputs from a Star Tracker (STA), four MEMS rate gyros, an Inertial Measurement Unit (IMU), and/or twelve Coarse Sun Sensors (CSS). It commanded spacecraft attitude and rotation rates, using four Reaction Wheels (RW) and four small Reaction Control System (RCS) thrusters. The RCS thrusters had control valves and latch valves which were commanded via a Valve Driver Unit (VDU). The change in velocity for large maneuvers was provided by the Orbital Control System (OCS), a large, single, fixed thruster positioned carefully so that the thrust vector was directed towards the center of mass.

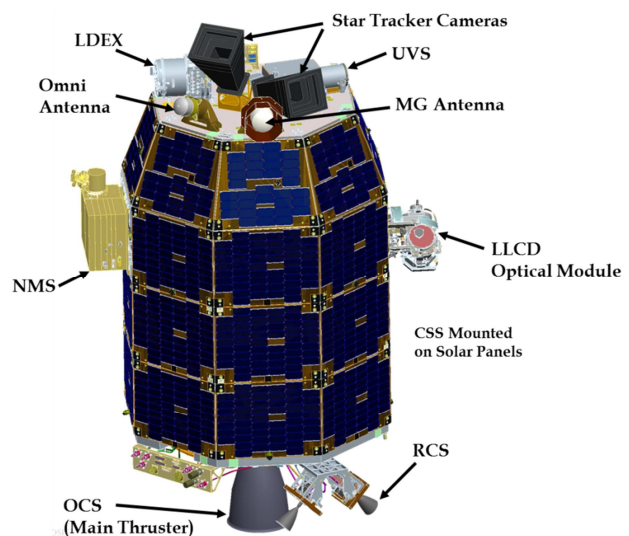


Figure 1 - LADEE Spacecraft Components and Payloads

Launched on September 7, 2013 UTC, LADEE completed a series of phasing loops and entered lunar orbit on October 6, 2013 UTC with the first of three Lunar Orbit Insertion (LOI) maneuvers. [3] The first LOI maneuver (LOI-1) was essential in order to be captured by the moon's gravity. Delaying this maneuver would have required extra propellant to achieve lunar orbit, therefore leaving less fuel to support science operations. Table 1 shows the impact to the mission for a delayed start of burn. A delay of more than 20 minutes would have made the mission unviable.

Table 1. Mission Impact from delayed LOI-1 Maneuver

Maneuver Delay (minutes)	Impact to Mission
5	Mission still meets most science objectives.
10	Mission meets many science objectives, but does not achieve full success.
15	Mission meets only minimum science objectives.
20 +	Mission does not meet science objectives.

The standard onboard automated fault management system that was used throughout the mission would have placed the spacecraft in a state that would have delayed or prevented the burn. Therefore most of the automated fault management responses were disabled during this critical period. Because the automated responses were disabled, the LADEE team needed to be fully prepared to execute LOI-1 even in the face of potential spacecraft faults. Therefore an analysis was conducted for the various types of contingencies that could occur, including component failures, inadvertent change to safe mode, inadvertent reboot, software failures, interrupted communications, and premature termination of the thruster burn.

For each likely contingency, the team readied detailed response procedures and command products that could be quickly executed if needed. This was followed by careful planning of the operations staffing, as well as rigorous testing of both the nominal and contingency scenarios. [7]

Ultimately, the LOI-1 maneuver was executed without incident. But this level of careful preparation was essential in ensuring the mission could succeed had a contingency arisen. This paper describes the analysis, design, and preparation for the LADEE LOI-1 contingencies, and offers some top level lessons learned about the process.

2. ONBOARD FAULT MANAGEMENT DESIGN

LADEE's Project philosophy dictated an acceptance of risk of a single-string spacecraft, while also allowing the development of capabilities to leverage certain functional redundancies. This drove the fault management design such that simple onboard logic encoded in the flight software would place the spacecraft in a power positive and thermally

safe mode, and rely on ground operators for detailed fault assessment and recovery response. However, for critical operations, such as LOI, this automatic transition into safe mode was avoided because the spacecraft would not have been in the desired configuration. In these situations, fault management was placed in a "report only" mode, relying on operators to react to failures occurring, rather than respond to spacecraft safing.

LADEE leveraged Government Off the Shelf (GOTS) software called the Core Flight System (CFS) developed by Goddard Space Flight Center. [6] The ability to use simple logic, which could be disabled, drove the project to use the CFS Limit Checker (LC) application. LC works by setting a threshold on a specific telemetry packet, termed the Watchpoint Table. As seen in Figure 2, Watchpoints, or simple threshold comparisons, are logically combined in the Actionpoint Table, to describe which actions are performed. This autonomous response sequence is stored in sets of Relative Time Sequences (RTS) and executed when the Actionpoint is evaluated as true. For critical operations, the Actionpoints were configured to be in the Passive state, causing an event to be displayed on the Operator's console instead of executing the RTS.

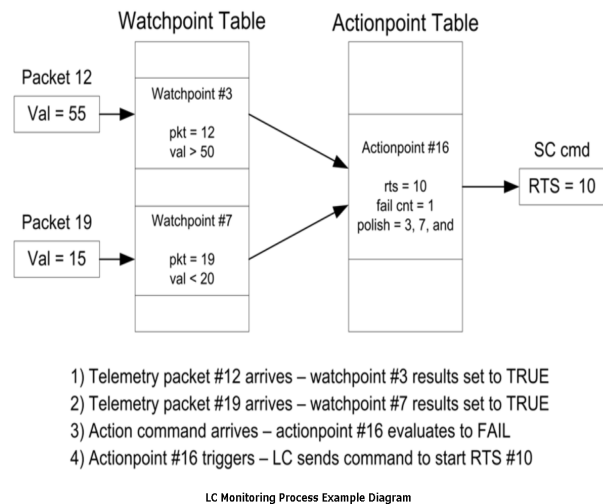


Figure 2 - Limit Checker Operation

The simple logic and execution frequency of the Limit Checker Application was not sufficient to protect against short time-to-criticality events. Therefore, LADEE also employed a set of safing actions within Flight Software. Specifically, the Fault Management design needed to protect against events such as CPU over usage, non-responding tasks, as well as the unlikely, yet possible, thruster leak.

Software failures were managed through the CFS module called Health and Safety (HS) which serviced a watchdog timer and provided a configurable response to non-responding tasks. The second column of Table 2 shows the

configuration of the HS table during normal operations. Upon detection of a non-critical task stopping, like the Payload IO services, HS would try to restart the app five times. After the fifth restart, the task would be stopped. For critical tasks such as Thermal and Power Control, HS would reboot the processor.

Table 2. Health and Safety Response for a Non-Responding Software Task

Task Types	HS response	
	Normal	LOI-1
Non-Critical Apps/ Payload Apps	Event	Event
Data Recording, Communication, GN&C Hardware I/O, Battery Charging	Restart	Restart
Fault Management	Reboot	Event
Scheduler	Reboot	Reboot
cFE Core	Event	Event
Safe Mode Control , Thermal control	Reboot	Restart
GNC Apps	Reboot	Reboot
State Estimator	Event	Reboot
Power Control	Reboot	Event

The second column of Table 2 shows the configuration of the HS table for the LOI maneuver. These modifications to the HS response represent a more benign response. However, in the case of the State Estimator task, the response changed from an event message to a processor reboot. The maneuver could not occur with an Estimator task restart because the spacecraft would not have enough knowledge of its attitude and thus would not guarantee a successful burn.

As shown in Table 3, fault management responses which were encoded within other FSW applications outside of the cFE layer, needed to be modified for LOI and other critical operations. These were modified in order to prevent a false positive error from triggering a fault management response.

3. DESIGN OF LOI CONTINGENCY OPERATIONS

The first part of the process for designing the contingency operations was to determine what spacecraft hardware was essential to the maneuver. This Minimum Equipment List (MEL) allowed the team to focus on what could go wrong with each device, and to look closely at what type of Failure Impact Workaround (FIW) might be used to mitigate the fault. The primary equipment identified in the MEL included the Reaction Wheels, Inertial Measurement Unit, Star Tracker, Latch Valves, RCS thrusters, OCS thruster, and Avionics/Software. Although it was highly desirable to maintain Spacecraft to Ground communications throughout the maneuver, it was not necessary for the actual burn to succeed because the entire maneuver was driven by onboard scripts.

Table 3. Specialized Flight Software Fault Management Modifications for LOI

Response	Purpose	LOI Modification
RCS Latch Valve Automatic Response	A leak in an RCS thruster could increase LADEE's angular rates quickly. FSW would close the latch valves to stop the leak.	Completely disabled via table modification
IMU Status Flags	IMU Hardware flagged internal faults.	Ignore IMU status flags. Let Estimator determine data validity.
Time to Divergence	The state estimator will diverge if it does not come up with a valid solution within a given time threshold.	The Estimator table was modified such that the time to solution divergence was inhibited.
Attitude Error	If the attitude error exceeds 10 degrees during a burn, then the control system will give up.	ACS maximum burn attitude error increased from 10 degrees to 180 degrees to take into account possible additional error due to cg shift.
Load Shedding	Under low voltage conditions, certain loads are shed to relieve the battery and allow quicker recharge.	Commands were sent to override the load shedding response for critical pieces of hardware needed for LOI.

In order to decide what failure workarounds to use and when to use them, the maneuver was divided into 6 distinct phases:

1. Normal Operations Prior to Reconfiguring Fault Management: the fault management response was unchanged from normal operations.
2. After the onboard fault management reconfiguration and prior to Loss of Signal (LOS) due to Lunar occultation: with most of the onboard fault management disabled, Mission Operations was responsible for monitoring the spacecraft subsystems and initiating responses to faults if they occurred.
3. Lunar occultation: with the spacecraft out of view, success depended primarily on the robustness of some redundant systems.
4. After Acquisition of Signal (AOS) and prior to the burn: this period was expected to be 5 minutes in duration. Due to the very short time duration, limited diagnosis could occur.

5. After Start of Burn: approximately 4 minutes in duration, there was little to no time for diagnosis of a fault, and a severe consequence for interrupting a burn in progress.
6. Burn Complete: normal fault management is

restored.

Table 4 lists the selected fault responses for each phase. Similar or related fault responses were grouped together in order to develop procedures and command products.

Table 4. Recoveries for each Phase of LOI

Fault	Recovery Normal	Recovery after FM Reconfig	Recovery After LOS	Recovery after AOS	Recovery During Burn
RW Failure	Recover manually from Safe Mode. ^A	Troubleshoot and try to bring back on line. ^B	Do Nothing. Rely on 3 wheel control.	Switch to DeltaV on-pulsing. ^E	Do Nothing. RW's not required.
IMU Failure	Recover manually from Safe Mode. ^A	Troubleshoot and try to bring back on line. ^B	Do Nothing. Rely on STA.	Switch to RW Gyros for rates. ^E	Do Nothing. No recovery likely to be effective.
STA Failure	Recover manually from Safe Mode. ^A	Troubleshoot and try to bring back on line. ^B	Do Nothing. Rely on IMU.	Do Nothing. Rely on IMU.	Do Nothing. Not needed during burn.
STA Blocked or Glare	Recover manually from Safe Mode. ^A	Do Nothing. Rely on IMU.	Do Nothing. Rely on IMU.	Do Nothing. Rely on IMU.	Do Nothing. Not needed during burn.
Latch Valve Fails closed.	Will not know.	Will not know.	Will not know.	Power cycle the VDU and repeat command. ^E	Do Nothing. No recovery likely to be effective.
RCS Leak	Recover manually from Safe Mode. ^A	Highly unlikely. Do Nothing.	Highly unlikely. Do Nothing.	Highly unlikely. Do Nothing.	Do Nothing. ACS will automatically compensate.
RCS Thruster Stuck	Will not know.	Will not know.	Will not know.	Will not know.	Do nothing. ACS will try to compensate.
VDUNo Response	Will not know.	Troubleshoot and try to bring back on line. ^B	Do nothing until spacecraft is in view.	Reset circuit breaker and power cycle VDU ^E	Power cycle VDU and restart burn. ^F
OCS Thruster Stuck Off	Will not know.	Will not know.	Will not know.	Will not know.	Power cycle VDU, and restart burn. ^F
CG shift during burn	Will not know.	Will not know.	Will not know.	Will not know.	Do nothing. Recovery not likely to be effective.
FSW Reboot	Recover from Safe Mode ^A	Modified bootup script prepares for burn. ^D	Modified bootup script prepares for burn. ^D	Modified bootup script prepares for burn. ^D	Modified bootup script prepares for burn. ^D
Comm Failure	Troubleshoot and try to bring back on line. ^C	Troubleshoot and try to bring back on line. ^C	Will not know.	Troubleshoot ground systems only. ^C	Troubleshoot ground systems only. ^C

Category Key

^A Normal Safe Mode Recoveries

^B Troubleshooting after FM Reconfig

^C Comm Issue Recoveries

^D Reboot Recovery

^E Specialized HW Failure Recoveries after AOS

^F Restart Burn Recovery

The categorizations grouped similar types of fault responses. These were useful in that they could be handled using similar methods and command products, and therefore could be represented as contingency branches within Real Time Operations (RTO) Procedures. Each of these categories is discussed in more detail in the sections that follow. The cells in the table that are not shaded correspond to contingency responses that were disqualified, either because they were infeasible, or because they were a lower priority.

Normal Safe Mode Recoveries

These fault responses corresponded to the same type of response that might be initiated at any other time during the mission. In general, the approach was to analyze the event log and housekeeping data to determine why safe mode occurred, and then to initiate a set of actions (not necessarily pre-planned) to correct or bypass the situation. After these actions were taken, the spacecraft would have been manually commanded out of safe mode and returned to normal operation.

Troubleshooting after Fault Management Reconfiguration

The Fault Management reconfiguration prevented entering safe mode when a fault occurred. Any problems that occurred after reconfiguration would need to be corrected while in the spacecraft's Fine Pointing mode. Normal troubleshooting steps could take place, as long as they did not interfere with or jeopardize the burn. For instance, if the VDU was not responding, then a power cycle of the VDU could have been executed since it was not actively used during this period.

Comm Issue Recoveries

In general, this type of recovery may have required troubleshooting the ground data systems, the network, and the ground station to re-establish communication. Troubles at the ground station may have been alleviated by switching to a backup station. If none of these were successful, a command could have been sent in the blind to try and power cycle the transmitter. This was disallowed after AOS to reduce the risk of interrupting the burn.

Reboot Recovery

Prior to Fault Management Reconfiguration, the Reboot Recovery would have been treated similarly to a Safe Mode recovery. After Fault Management reconfiguration, there still existed a possibility that a fault could occur which would trigger an automated response to reboot the processor, such as the expiration of the watchdog timer.

The approach to a reboot was to modify the onboard default RTS that executed immediately after startup. Its normal operation was to put the Limit Checker in an active state, which would detect the state of the spacecraft, power on devices, and cause the system to go into Safe Mode. Normally, Safe Mode would have been desirable after a reboot to keep the spacecraft thermally safe and power

positive. But for LOI-1, it would have altered the spacecraft attitude away from the burn attitude, and hence prevented the burn.

For LOI-1, the default RTS was modified to eliminate enabling the Limit Checker. Instead, it executed additional RTSs that powered on the devices, and then immediately executed commands to set up for the burn – including the command to orient to the burn attitude. Once in view, a manual command could have been sent from the ground to execute the burn.

Specialized Hardware Failure Recoveries after AOS

There were a number of hardware faults for which there were specialized responses that could either correct or circumvent the problem. After AOS there was little time to diagnose and correct a problem before the burn occurred. Therefore, detection and diagnosis of these problems corresponded to monitoring very specific telemetry points for a particular signature. If one of these problems was identified, then a pre-defined onboard RTS would have been executed to try to correct the problem.

Restart Burn Recovery

If the burn should have started but for some reason failed to execute, then every minute that passed by before reattempting the burn would have increased the amount of propellant usage to achieve capture. Therefore, the burn signature was monitored very closely to ensure that the burn was actually taking place. If the burn signature was not observed, or if the signature indicated that the burn stopped prematurely, then action would be needed to restart the burn. Fortunately there were 5 clear telemetry signals that could be monitored to detect the burn. Given the severe consequence of stopping a good burn based on bad sensor data, at least 4 of the 5 signatures were required to indicate an error before action was to be taken.

The failures that would have prevented or stopped the burn itself were a very short list. Therefore, all of the actions to correct all of these failures would have been executed without needing to conduct a diagnosis on which occurred:

1. Something went wrong in the sequence – Stop the sequence.
2. The VDU Circuit Breaker tripped – Reset the breaker.
3. The VDU had an Internal Fault – Power cycle the VDU.
4. The OCS coil is bad – Switch to the Redundant Coil.
5. The Fire Command was not received - Run the Burn sequence again

Based on this list of scenarios, the detection and resulting actions could have occurred within a few minutes, and thus salvaged the mission. If the burn already started, and the

telemetry signatures showed that the burn stopped, the same actions could be taken to restart the burn.

4. CONTINGENCY PROCEDURES PREPARATION

Based on the contingency operations design, procedures were developed to cover the fault categories described. The timeline for when contingency procedures were in effect is shown in Figure 3. Note that there were some modifications that were implemented after the initial design. For instance, the Special Hardware Recoveries procedure went into effect prior to going out of view since time would have been short to do standard troubleshooting. Also, an additional contingency category was added called State Estimator Recovery. During operations, it was noted that in certain circumstances, a bright object in the field of view of the star tracker could cause the estimator to diverge resulting in an unknown spacecraft attitude. If this situation was detected, the estimator would need to be re-initialized to correct the problem.

To ensure the success of the fault management reconfiguration and contingency preparations the following

precautions were taken:

- All of the preparation and reconfiguration was implemented via reviewed, tested, and approved scripts so that it was executed exactly as it was practiced each time.
- LOI-1 preparations were conducted well in advance of the maneuver to ensure there was plenty of time to get it accomplished, even in the face of unforeseen difficulties.
- Many of the contingency responses were to be executed via RTS so that they could be executed quickly via a single ground command. These specialized RTSs were uploaded and enabled during the preparation phase.
- To prepare for the reboot contingency, a special boot image was created that included all of the contingency RTSs, modified tables, and modified default RTS. After the burn, the fault management was reverted to its normal configuration, and the

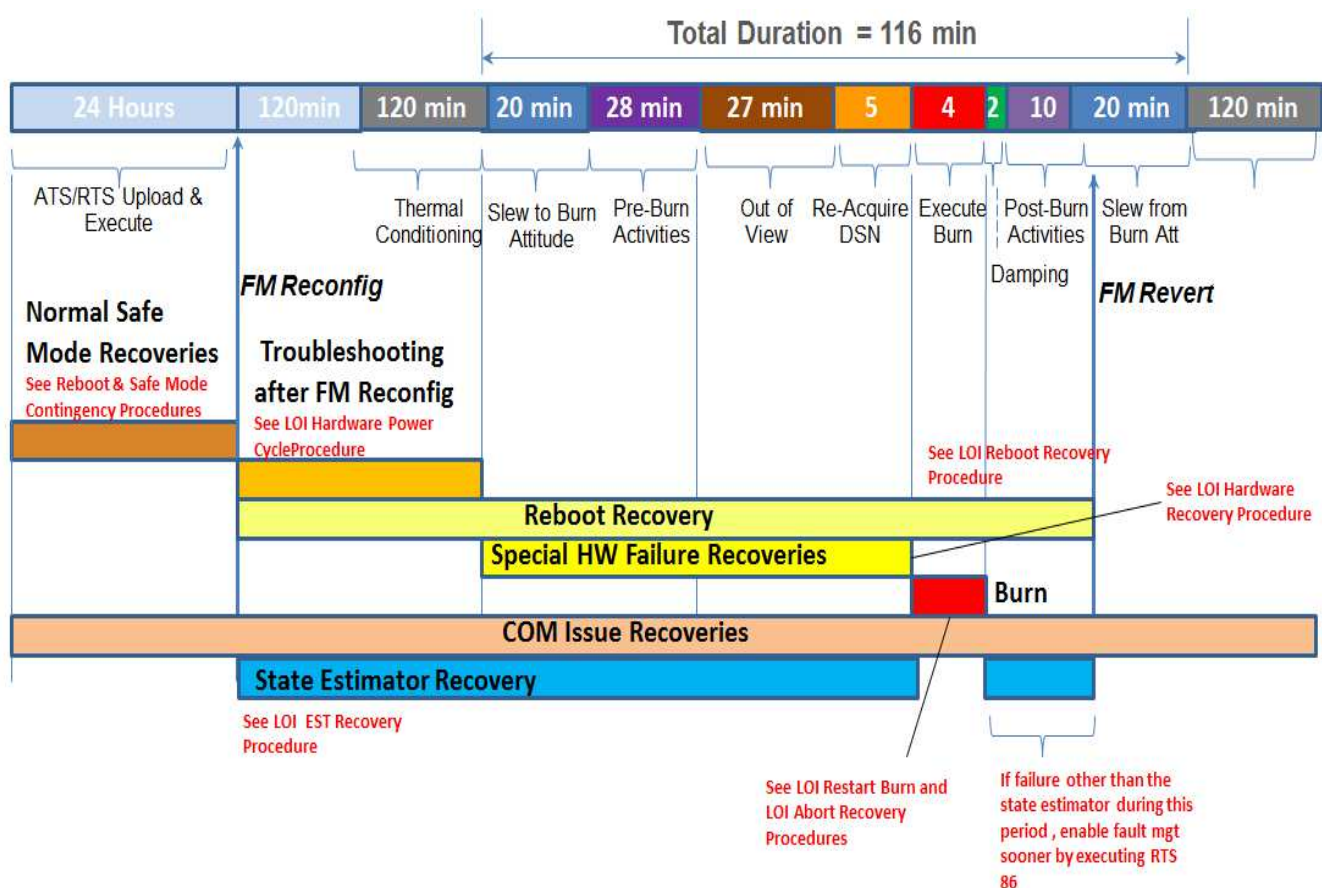


Figure 3 - Timeline for Contingency Procedures

boot image pointer was set to the default boot load.

Note that the creation of an alternate boot image for LOI was viewed as a lower risk approach than modifying the default boot image. The likelihood of a reboot occurring was relatively low for the short period of time leading up to LOI-1. However, if a mistake was somehow made in the configuration of the default image, then over the longer term a reboot would be more likely, and a corrupted default image could result in severe consequences. Therefore, it was less risky for the overall mission to create an alternate boot image, and discard it after LOI. The alternate boot image was created in flight by copying the object files, RTSs, and tables from the spacecraft's memory, replacing the files needed to support the reboot contingency, and then installing these into the new boot partition. The process was done in flight to ensure that the alternate image would contain all of the latest files in use onboard the spacecraft. [8]

5. MISSION OPERATIONS STAFFING

The on-console mission operations team was expanded to support LOI execution. For a non-maneuver day, real-time mission support staffing was limited to three console positions – the Flight Director, a Systems Engineer, and a Command Controller. For typical non-critical maneuvers, this staffing expanded to include the Mission Operations Manager (MOM), a Data Engineer, a trajectory analyst, and a supporting Spacecraft Engineering Team (SET). The SET included separate support engineers for each spacecraft subsystem – Avionics, Communications, Electrical, GNC, Propulsion, and Thermal. For LOI, this maneuver team expanded to include a second System Engineer and a Mission Planner. The role of this second Systems Engineer was to monitor for fault conditions identified in the procedures, and to make recommendations to the Flight Director whether to execute one of the contingency procedures. The role of the Mission Planner was to provide assistance in recommending or building command products if required.

In addition to mission operations console staffing, Project Management and Safety & Mission Assurance representatives were present for all maneuvers, including LOI. More details about LADEE's operations and staffing approach can be found in [5].

6. TESTING AND TRAINING

All aspects of LOI planning, preparation and execution were practiced before launch; some portions of this sequence were also rehearsed during flight days prior to LOI execution. These practice sessions took three forms – mission simulations, Operational Readiness Tests (ORTs) and rehearsals – and demonstrated abilities to respond to both spacecraft and ground system anomalies during LOI operations. Prior to each of these practice activities, the

Mission Operations team would hold pre-briefs to review procedure steps and discuss contingency scenarios.

Mission simulations provided the first integrated simulation environment in which to exercise all aspects of a mission activity. Where previous “thread tests” involved only one or two operations personnel and exercised individual tools or products, simulations generally involved the entire operations team, all operations tools and all products required to perform an integrated activity such as a maneuver. As a first step in testing and practicing an activity, simulations often identified problems such as errors in procedures, flaws or weaknesses in tools, and areas in which personnel required further training. In general, simulations focused on nominal operations rather than response to failures. For LOI, however, mission simulations included practice of contingency responses as outlined in LOI-specific flight procedures. These included major spacecraft anomalies, such as spacecraft reboot and temporary loss of propulsion system control, and ground system anomalies including loss of Deep Space Network ground station functions and failover of Mission Operations Center data systems.

After mission simulations were completed, ORTs served as formal tests to validate the approaches developed and refined through those mission simulations. ORTs were executed to be as flight-like as possible, even executing simulated activities at the same time of day as planned during the mission. The LOI ORT lasted 4 days, encompassing not only fault management reconfiguration and maneuver execution, but also the post-maneuver process of orbit determination and planning for the next maneuver. All ORTs addressed contingency scenarios; the LOI ORT included response to temporary loss of Star Tracker function, transient memory errors in LADEE's flight computer, and failures in the Mission Operations Center data system.

Rehearsals provided a final opportunity – in the final weeks prior to launch – to practice procedure execution, timing, and team coordination for key events including launch and activation, phasing maneuvers and LOI. A two day LOI rehearsal allowed practice of the sequence of preparation, execution and recovery. A final rehearsal was performed post-launch, approximately two weeks prior to LOI-1 execution. This rehearsal exercised the nominal operations plan for thermal conditioning and maneuver execution only. No malfunctions were simulated as a part of this rehearsal.

More details about the LADEE testing process can be found in [4].

7. OUTCOME AND CONCLUSION

Fortunately, the LOI-1 maneuver succeeded without any issues, and the contingency procedures were not utilized. However, the team was well prepared to have handled any

of these situations. This was accomplished through a thorough development and preparation process addressing the onboard fault management system configuration, contingency procedures, command products, staffing levels, and training.

Based on the LADEE team's experiences with this preparation, the following high level recommendations are offered to other missions facing similar circumstances:

1. We recommend a methodical approach for developing contingency operations for critical activities. Shortly stated, the approach used on LADEE was:
 - a. Create a Minimum Equipment List and Failure Impact Workaround study.
 - b. Divide the activity into phases.
 - c. Triage the failures and workarounds in each phase based on risk, to decide on which contingencies to address.
 - d. Group similar contingencies in order to create procedures and supporting command products.
 - e. Ensure an appropriate level of staffing is available in operations to handle both nominal and contingency situations.
 - f. Ensure the staffing is well trained through repeated testing of both the nominal and contingency situations.
2. We recommend that missions develop the Minimum Equipment List and Failure Impact Workaround study as early as possible and in conjunction with the development of the fault management plan. Early development allows trades to be made in how fault mitigation is handled, either through hardware, software, or operations. When making changes to the system design, these studies should be revisited and impacts assessed.
3. Practicing both nominal and contingency scenarios by the operations and engineering staff was invaluable for familiarizing the team with the processes, products, and procedures. In addition it was a useful means for getting feedback and honing these items. Therefore it is desirable to do this testing as early as possible, including as much of the engineering and operations staff as practical.

ACKNOWLEDGMENTS

The authors would like to thank all of the members of the LADEE project team.

This work and the LADEE mission was performed at the NASA Ames Research Center, under the Lunar Quest Program, and sponsored by the NASA Science Mission Directorate Division of Planetary Science.

REFERENCES

- [1] Delory, G.T.; Elphic, R.; Morgan, T.; Colaprete, T., Horanyi, M.; Mahaffy, P.; Hine, B.; Boroson, D., "The Lunar Atmosphere and Dust Environment Explorer (LADEE)", 40th Lunar and Planetary Science Conference, (Lunar and Planetary Science XL), held March 23-27, 2009 in The Woodlands, Texas, id.2025.
- [2] Butler P. Hine, Stevan Spremo, Mark Turner, and Robert Caffrey, "The Lunar Atmosphere and Dust Environment Explorer Mission," 2010 IEEE Aerospace Conference Proceedings, March 6-13, 2010.
- [3] Arlen Kam, Laura Plice, Ken F. Galal, Alisa M. Hawkins, Lisa A. Policastri, Michel E. Loucks, John P. Carrico, Craig A. Nickel, Ryan L. Lebois, and Ryan Sherman, "LADEE Flight Dynamics: Overview of Mission Design and Operations," 25th AAS/AIAA Space Flight Mechanics Meeting Proceedings, January 11-15, 2015.
- [4] Brandon D. Owens and Alan R. Crocker, "SimSup's Loop: A Control Theory Approach to Spacecraft Operator Training," 2015 IEEE Aerospace Conference Proceedings, March 7-14, 2015.
- [5] Matthew V. D'Ortenzio, John L. Bresina, Alan R. Crocker, Richard C. Elphic, Ken F. Galal, David R. Hunt, Brandon D. Owens, Alisa M. Hawkins, Laura Plice, and Lisa A. Policastri, "Operating LADEE: Mission Architecture, Challenges, Anomalies, and Successes," 2015 IEEE Aerospace Conference Proceedings, March 7-14, 2015.
- [6] McComas, David, "NASA/GSFC's Flight Software Core Flight System", Flight Software Workshop, <http://flightsoftware.jhuapl.edu/>, 2012.
- [7] Nathaniel A. Benz, Danilo Viazzo, and Karen Gundy-Burlet, "Multi-Purpose Spacecraft Simulator for the LADEE Mission," 2015 IEEE Aerospace Conference Proceedings, March 7-14, 2015.
- [8] Gundy-Burlet, Karen. "Maintenance Phase Considerations for Onboard Flight Software Development", SciTech 2015, Kissimmee FL, Jan 5-9, AIAA-2015-1875.

BIOGRAPHY



Howard Cannon is a Computer Engineer at NASA Ames Research Center. He served as the Flight Software Subsystem Lead throughout most of the LADEE spacecraft development phase. He then served as a Flight Director in Mission Operations for the remainder of the mission. He led the development of the LOI contingency operations effort in Mission Operations, and was on console as a Systems Engineer during the LOI maneuver. Cannon has a B.S. in Mechanical Engineering from Bradley University in Peoria IL, and an M.S. in Robotics from Carnegie Mellon University.



Anupa Bajwa is a researcher in the Intelligent Systems Division at Ames Research Center. She is the Project Manager for Autonomous Systems, a project of NASA's Game Changing Development Program. She led the Fault Management team for the LADEE mission. She previously worked on implementing Integrated Systems Health Management (ISHM) for launch vehicles on projects such as PITEK, Space Launch Initiative, and Constellation. She holds a doctorate degree in Aerospace Engineering from the Pennsylvania State University, and is a recent graduate of NASA's Mid-Level Leader Program



Peter Berg Peter Berg is a Research Engineer with Stinger Ghaffarian Technologies at NASA Ames Research Center. He served as Flight Software System Engineer, Fault Management Engineer, Simulation Engineer, and as the System Engineer flight controller for LADEE. Presently, he works with the Mission and Fault Management Team for the Space Launch System. He is a member of the NASA Engineering and Safety Center's Software Discipline Team. Peter has a B.S. in Aerospace Engineering from Embry-Riddle Aeronautical University.



Alan R. Crocker serves in the Chief Engineer's Office at NASA Ames Research Center. Previously, he served in several roles at the NASA Johnson Space Center. He has supported human and robotic space exploration projects as a systems engineer, flight controller, instructor, team lead, manager and instructor. For the LADEE mission, he formed and led the mission operations spacecraft engineering team. He received a B.S. in Aeronautical and Astronautical Engineering from Purdue University and is a graduate of NASA's Systems Engineering Leadership Development Program.

APPENDIX A: ACRONYMS

AOS	Acquisition of Signal
CFS	Core Flight System
CSS	Course Sun Sensors
FIW	Failure Impact Workaround
GNC	Guidance, Navigation, and Control
GOTS	Government Off-The-Shelf
HS	Health and Safety (a CFS application)
IMU	Inertial Measurement Unit
LADEE	Lunar Atmosphere and Dust Environment Explorer
LC	Limit Checker (a CFS application)
LDEX	Lunar Dust Experiment
LLCD	Lunar Laser Communication Demonstration
LOI	Lunar Orbit Insertion
MEL	Minimum Equipment List
MEMS	Micro-Electro-Mechanical System
MOM	Mission Operations Manager
NMS	Neutral Mass Spectrometer
OCS	Orbital Control System
ORT	Operational Readiness Review
RCS	Reaction Control System
RTO	Real Time Operations
RTS	Relative Time Sequence
RW	Reaction Wheels
SET	Systems Engineering Team
STA	Star Tracker Assembly
VDU	Valve Driver Unit

