NASA/CR-2005-213472

Preliminary Report on Mission Design and Operations for Critical Events

Sandra C. Hayden, Irem Tumer

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California, 94035-1000

December 2005

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the Lead Center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at (301) 621-0134

- Telephone the NASA Access Help Desk at (301) 621-0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076-1320

NASA/CR-2005-213472

Preliminary Report on Mission Design and Operations for Critical Events

Sandra C. Hayden
QSS Group, Inc., NASA Ames Research Center, Moffett Field, CA

Irem Tumer
NASA Ames Research Center, Moffett Field, CA

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California, 94035-1000

December 2005

Available from:

NASA Center for AeroSpace Information
7121 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

TABLE OF CONTENTS

1 Scope

Mission-critical events are defined in the Jet Propulsion Laboratory's Flight Project Practices [7] as those sequences of events which must succeed in order to attain mission goals. These are dependent on the particular operational concept and design reference mission, and are especially important when committing to irreversible events. Critical events include main engine cutoff (MECO) after launch; engine cutoff or parachute deployment on entry, descent, and landing (EDL); orbital insertion; separation of payload from vehicle or separation of booster segments; maintenance of pointing accuracy for power and communication; and deployment of solar arrays and communication antennas. In each of these events, critical functionality is provided by the major subsystems (e.g., propulsion, power, communication, attitude control, and life support) and a failure in one or more subsystems may lead to mishap.

The central objectives of the Critical Event Insight Task are to:

- Report on the current practices in handling mission-critical events in design and operations at major NASA spaceflight centers
- Report on recommended best practices for mission design and operations for critical events

This report addresses the first objective. The scope of the report includes NASA Johnson Space Center (JSC), NASA Goddard Space Flight Center (GSFC), and NASA Jet Propulsion Laboratory (JPL), with staff at each center consulted on their current practices, processes, and procedures. These centers were chosen based in part on their strong mission focus, and on available contacts.

A major operations phase of an active mission has been selected at each center: rendezvous and docking operations for Space Shuttle with Space Station at JSC; on-orbit operations for remote sensing satellites at GSFC; and surface operations for Mars exploration rovers at JPL. For each mission, critical events will be identified and analyzed in this report. In addition, mission design and operations practices and procedures that support critical events at each center will be explored.

A follow-on report will address the second task objective. The approach will be to make recommendations on principles and best practices to identify the intersection between critical events, system functions, and observable state variables that will support anomaly resolution and other decision making relative to system performance. The follow-on report will also be a preliminary report; it is to be expected that a more formal, binding report would require extensive further work with NASA centers to develop a set of agreed-upon best practices, and that is beyond the intended purpose of this informal report.

1.1 Purpose

The Critical Event Insight Task was generated in response to the Diaz Team Report Actions (see the Diaz Report [1] and the Columbia Accident Investigation Board Report [2]). Related Diaz Actions are:

- Review/develop current policy or guidance that assures critical event data is collected, observed, and analyzed

- Develop a standard for comprehensive program risk management and observable data collection for all phases of program development, test, operation, and enhancement to be used for program management, improvement, and anomaly/disaster reconstruction
- Identify methods used by other test organizations to perform remote system testing and anomaly resolution

1.2 Terminology

For the purposes of this report, *critical events* are defined as those events that must be successful, in order to meet mission goals. This meets the JPL definition of the term. GSFC and JSC generally understand the concept of a critical event to mean an anomaly or hazardous condition. The distinction to be made is that *anomalies* are failures that may or may not involve critical events. Failed critical events result in *mishaps*. In the worst case, an anomaly compromises achievement of mission objectives and hence the critical event, resulting in a mishap. Mishaps are catastrophic failures often categorized as loss of mission (LOM), loss of vehicle (LOV), or loss of crew (LOC).

A distinction may also be made between "hard" critical events and "soft" critical events. Hard critical events have irreversible consequences (mishaps) should the critical event fail. Soft critical events have reversible consequences and hence may be recoverable. Should a soft critical event fail, the result is a system anomaly and disabled or impaired functionality required to meet mission goals, with the possibility of a workaround requiring intervention.

Other related concepts are *flight rules* and *safety rules*, which are procedures developed to ensure successful completion of critical events.

2 The Role of Critical Events in NASA Mishaps

A Mishap Cause Classification (MCC) study [11] identified recurring problem areas and trends in NASA mishaps, through the systematic analysis and classification of causes across a representative set of mishaps. The approach used was to develop and apply a classification method and taxonomy of systemic causes of mishaps, and of subsystems and cross-system elements involved in mishaps. Management Oversight and Risk Tree (MORT) was used as the basis for the mishap cause taxonomy.

Analysis of 21 mishaps yielded the most frequently cited categories of mishap cause (insufficiencies in design, test, and management processes; limitations of human performance and procedure implementation), as well as the subsystems most often involved (structures and mechanisms, propulsion, control, guidance, and navigation). The cross-system elements most frequently cited were subsystem interactions, software, humans-in-the-loop processes, materials, and the environment. Trends were identified suggesting that unintentional subsystem interactions have become a significant cause of mishaps since 1997, and that design problems have remained consistently high since 1995.

This report looks beyond mishaps, encompassing critical events during nominal and anomalous operations that have the potential to lead to mishaps. The focus of the analysis is shifted to the moments before committing to the fatal event. At the GO/NO-GO checkpoint for the critical event, this is the last chance to assess the pre-commit criteria and inform the decision whether it is safe to continue.

The approach used is to identify the critical event that failed for each mishap; list the pre-commit criteria in terms of measurements or telemetry readings that formed the basis for the decision; list the desired state of those parameters after the critical event, had it been successful; and finally show the actual outcome of the mishap in terms of anomalous parameters, as well as the root cause fault and implicated subsystem(s) or functionality that failed. Table 1 below catalogues several NASA mishaps in terms of their critical events. Mishap reports comprehensively document the Mars Polar Lander [3], Mars Climate Orbiter [4], Mars Observer [5], CONTOUR [6], NEAR [18] and Challenger [19] mishaps.

The question is: *what were the missing criteria or anomaly detection capabilities that would have prevented a "GO" decision,* if any, with its irreversible consequences. In many cases, the system is under-sensed and could not provide these distinguishing measurements. For example, the hydrogen leak in the SSME nozzle tubes could have been detected by an on-board optical plume anomaly detection (OPAD) system. In some cases, the decision could have been supported by piecing together existing information from a variety of sources, such as the Mars Polar Lander premature engine cutoff due to a faulty sensor that indicated touch-down. A check of altimeter or system state, deploying legs, could have prevented engine shutoff at 40 meters above the Martian surface.

All of these mishaps relate to propulsion. Orbital insertion/departure proved the most hazardous mission phase, followed by launch and EDL. System engineering appears as a cause in more than half of these cases, in agreement with the MCC study's most frequently cited cause as "insufficiencies in design, test, and management processes." However this sampling is statistically too small to be representative of NASA missions in general.

Table 1: Critical Events and Outcomes in Mishaps

Critical Event (CE)	Mission Phase	Measurement	Pre-CE Commit	Desired Post-CE, Nominal	Actual Post-CE, Anomalous	Root Cause	Subsystem(s) / Function	Mishap Case
Main Engine Cut-Off (MECO)	Entry, descent and landing (ED&L)	• Hall effect sensor on landing gear. • Radar altimeter (data not utilized).	• Touchdown Monitor (TM) indicates spacecraft has landed. • Safe landing altitude (not utilized due to inaccuracy?)	Touchdown and MECO.	Premature MECO at altitude, spacecraft destroyed.	C&DH commanded MECO based solely on Touchdown Monitor, which indicated falsely during transient of landing gear leg deployment.	• Subsystems: C&DH, landing gear • System Engineering: Failure to flow down requirement to disable TM during leg deployment • System Engineering: pre-commit for CE did not assess altitude, verify touchdown. Also not state aware: that the legs are being deployed, pre-touchdown.	Mars Polar Lander (MPL)
MECO	Launch	• Fuel pressure • Oxidizer pressure	TBD	MECO at target altitude	Premature MECO.	Hydrogen leak in nozzle tubes	Space Shuttle Main Engine (SSME)	STS-93
Rocket burn	Launch	None.	TBD	Nominal delta-V	Shuttle destroyed	O-ring failure, structural overheating from SRM plume	Solid Rocket Motor (SRM)	Challenger STS-51L
Rocket burn	Orbit departure from Earth to comet Encke	None.	TBD	Nominal delta-V	Spacecraft destroyed	Structural overheating from SRM exhaust plume, temperatures high enough to melt some components	• SRM • System Engineering: SRM nozzle was embedded within the spacecraft to a greater degree than is typical • Temperature/structural sensors. For throttle-able engine, might have aborted to slow burn	CONTOUR (Comet Nucleus Tour)
Rocket burn	Orbit insertion around the asteroid Eros	Accelerometers (lateral acceleration)	TBD	Nominal delta-V	• FP software aborted the burn. • Tumbling spacecraft, thrusters fired thousands of times, wasting fuel	• SRM's normal start-up transient exceeded a lateral acceleration safety threshold. • Missing command in the burn-abort contingency command script started the attitude anomaly.	• SRM • System Engineering: safety threshold set too low for this spacecraft design. • System Engineering: script error in burn-abort, thrusters selected instead of reaction wheels	NEAR (Near Earth Asteroid Rendezvous)
Propulsion system helium pressurization	Orbit insertion around Mars	• Monomethyl hydrazine (MMH) fuel pressure • Nitrogen tetroxide (NTO) oxidizer pressure	Nominal fuel and oxidizer pressures, pre-pressurization (low)	Pressurized rocket thruster fuel, oxidizer tanks	Reaction of NTO and MMH ruptured tubing. Leaking He and MMH put the spacecraft into a catastrophic spin.	NTO leaked through check valves into the pressurization tubing.	Propulsion Feed System	Mars Observer
Angular momentum management	Orbit insertion around Mars	Thruster performance data (small forces delta-V's)	TBD	Angular Momentum Desaturation (AMD)	An erroneous trajectory was computed using incorrect data.	Small forces delta-V's too low, provided in English units instead of metric units. Underestimated the effect on the spacecraft trajectory by a factor of 4.45.	System Engineering: Software Interface Specification (SIS) not met, failure to provide data in metric units for trajectory calculation, per requirements	Mars Climate Orbiter (MCO)

3 Critical Events at NASA Johnson Space Center

3.1 JSC Mission Design Practices

The focus of JSC is on operation of human spaceflight for Space Shuttle and International Space Station (ISS). JSC therefore does not require the equivalent of the GSFC Gold Book or the JPL Flight Project Practices handbook, which specify practices and procedures for the design, development, and verification of flight systems.

3.2 JSC Operations Procedures

The JSC Mission Operations Directorate (MOD) and the Flight Director Office govern Shuttle and ISS operations through a series of Flight Rules documents. These are the "Generic All Flights Books":

- Volume A - "Space Shuttle Operational Flight Rules"
- Volume B - "ISS Generic Operational Flight Rules"
- Volume C - "Joint Shuttle/ISS Generic Operational Flight Rules"
- Volume D - "Soyuz/Progress/ISS Joint Flight Rules"

In order to focus the discussion, this section concentrates on the preparation for and handling of critical events for ISS as documented in volumes B and C, "ISS Generic Operational Flight Rules" and "Joint Shuttle/ISS Generic Operational Flight Rules."

The process for development of JSC operations procedures is as follows. The JSC program office utilizes a Hazard Analysis process to identify and analyze critical events. The program office and vendors determine potential hazards and document these in Hazard Reports. For example, a hazard report may specify the risks of a space shuttle Reaction Control System thruster plume impacting an ISS solar array during docking, thereby damaging or breaking the solar array. These hazard reports are flowed down to the MOD to identify and implement appropriate Operational Controls such as specific procedural steps (turn the solar arrays away from the plume), Flight Rules (verify that the solar arrays are turned away), and/or crew training (check solar array orientation before approaching within 400 ft of ISS).

Examples of critical events for ISS, identified in this hazard analysis process, include:

- Attitude handover - transition from use of Russian attitude control capabilities to US attitude control capabilities (and vice versa)
- Shuttle docking - reconfiguration of systems to withstand shuttle thruster plumes and impact forces of shuttle docking
- Command and Control Modulator/Demodulator (MDM) transition - handover of primary control of the vehicle from one computer to another
- Software uplink - update to onboard software by transmitting software patch to onboard mass storage, subsequent transfer of the software image to an MDM that is not in primary control of vehicle systems, followed by handover of primary control to that MDM

3.3 JSC Critical Events for Rendezvous and Docking of Space Shuttle with ISS

As the full suite of operations procedures and flight rules for ISS is enormous, the following analysis focuses only on critical events involved in the rendezvous and docking operations for Space Shuttle with ISS. Flight rules from the JSC docking operations policy are listed in Appendix A – JSC Rendezvous Operations Procedures. The following flight rules impose constraints associated with rendezvous and docking:

- C2-56 - Shuttle Go-No Go for Docked Operations
- C2-101 - ISS Go-No Go Matrix for Rendezvous
- C2-104 - ISS System Management for Approach and Dock
- C2-105 - Shuttle Sensor Requirements for ISS Proximity Ops

These rules, in turn, reference other flight rules which are not included here, that define required configurations prior to execution of docking operations.

Flight rules in C2-56 govern continued Shuttle docked operations. The major constraint that must hold is that, while docked, Shuttle must retain sufficient propellant for emergency undocking and de-orbit to the nearest landing site. C2-105 flight rules cover sensor needs to ensure safe Shuttle approach to ISS, such as redundant ranging devices including hand-held LIDAR (Light Detection and Ranging) to measure distance, speed, and rotation of Shuttle relative to ISS.

Criteria for successful completion of docking are at least partially addressed in flight rule C2-104. C2-104 (A) has procedures for ISS appendage configuration, specifically to ensure that the solar arrays are out of the line of approach. Thruster or external venting plume impingement can create adverse and unpredictable structural torques and unacceptable localized heating, as well as contaminate critical surfaces and degrade material properties.

C2-104 (B) states that micro-switches on ISS and Shuttle must detect that the docking mechanism has contacted. That, in turn, causes the vehicles to go to free drift (no attitude control). Free drift condition is required to ensure that neither vehicle applies forces or torques to the docking mechanism before it is ready. There are other actions and criteria after this to ensure that the two vehicles are completely mated and a good pressure seal exists between them, but these are excluded from this analysis.

Critical events for ISS rendezvous and docking are analyzed in Table 2. The flight rules are correlated to GO/NO-GO checkpoints, and broken down according to different possible operational scenarios. Pre-commit criteria for nominal (GO) conditions and anomalous (NO-GO) conditions are identified. Expected nominal post-commit conditions and anomalous post-conditions with recovery procedures, where supported, are identified. Telemetry or measurements which are the basis for the pre-commit criteria are identified. The overall mission phase that the critical event applies to, and any other related flight rules for this critical event, are specified. Finally, systems and subsystems involved in the interaction are identified. As expected, all of these events show interactions between subsystems, as well as interactions between systems.

Table 2: JSC ISS Rendezvous and Docking Critical Events and Corresponding GO/NO-GO Determinants

JSC Flight Rule	System	Mission Phase	Critical Event	Subsystem	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomalous Pre-Commit (NO-GO)	Anomalous (NO-GO) Recovery	Correlated Critical Events
C2-56	Orbiter	Docked Operations	Go/No-Go Continue Docked Operations	Propulsion (OMS, Forward RCS, Aft RCS)	OMS fuel/oxidizer levels FRCS fuel/oxidizer levels ARCS fuel/oxidizer levels	OMS propellant levels above redline FRCS propellant levels above redline ARCS propellant levels above redline	Continue Docked Operations.	1. OMS propellant below redline OR 2. FRCS propellant below redline OR 3. ARCS propellant below redline	Emergency undocking, separation, and deorbit to next primary landing site (up to 24 hours away).	Rule C4-152 Rule A6-303A, OMS Redlines. Rule A6-304A, FRCS Redlines. Rule A6-305, ARCS Redlines.
C2-104 A	ISS	Approach and Dock At PMA2 on the Lab Forward CBM	ISS appendage configuration	Solar arrays: P6 4B, P6 2B (USOS) FGB, SM (RS)	P6 4B solar array position. P6 2B solar array position. FGB solar array position. SM solar array position. Range between Orbiter and ISS.	To approach within 400 ft: P6 4B at 210° ±5°. P6 2B at 150° ±5°. To approach within 170 ft: FGB fixed in Sun Zone 1 or 9 SM fixed in Sun Zone 1 or 9 Approach within 1000 ft requires Low Z braking.	No change.	Solar arrays are not in position. Orbiter delays approach for up to one orbit to RETRY.		Rule C2-109 Orbiter Z braking must meet C2-109 rules. No Norm Z braking within 1000ft.
C2-104 B	ISS	Approach and Dock	Attitude Control at Docking	Attitude Control System (ACS). ISS-Orbiter communication. MMC-Orbiter communication	Capture indicator (Orbiter crew). ISS ACS mode indicator. Can be provided by: 1. ISS crew 2. Orbiter crew using LED dock indicators 3. MCC-H/MCC-M Command source availability indicators: 1. Automatic ACS moding by CCS (primary). 2. ISS crew (secondary backup) 3. MCC-H or MCC-M (tertiary backup)	Capture unconfirmed. ISS is in attitude control mode (LED steady on). At least one command source is available.	Capture confirmed. ISS ACS mode is free drift (LED flashing).	Capture -5 minutes: Automatic ACS moding by CCS not available (e.g. MDM failure).	If ACS moding by CCS not available, use backup. May need to wait 20 seconds, to prevent simultaneous commanding by several sources. ISS ACS mode is not free drift at: 1. Capture +20 seconds: RETRY using backup command source. 2. Capture +65 seconds: ABORT. Orbiter crew opens docking latches, performs 'Failed Capture Procedure'. ABORT prevents exceeding docking mechanism load limits.	Ground Site contact Flight Rule C2-106.

JSC Flight Rule	System	Mission Phase	Critical Event	Subsystem	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomalous Pre-Commit (NO-GO)	Anomalous (NO-GO) Recovery	Correlated Critical Events
C2-104 C	ISS	Approach and Dock	Approach and Dock	Communication	Telemetry antenna tracking mode	Ku-band in autotrack mode. Antenna "shuttle mask" enabled.				
C2-104 D	ISS	After Docking	Resume Sun Tracking	Solar arrays. Power.	Capture indicator (Orbiter crew). ISS ACS mode from: 1. ISS crew 2. Orbiter crew using LED dock indicators 3. MCC-H/MCC-M ISS Power	Capture confirmed. ISS ACS mode is free drift (LED flashing). Solar arrays fixed in approach configuration (not sun tracking). ISS Power down for rendezvous	Solar arrays are sun tracking. ISS Power charging from arrays.			
C2-104 E	ISS	Approach and Dock	Observe docking procedures from U.S. Lab	US Lab	U.S. Lab window Shutter	U.S. Lab window Shutter may be down	U.S. Lab window Shutter up	Shutter fails in lowered position.		Rule B2-19
C2-105 A	Orbiter	ISS Proximate Operations	Shuttle Sensors Required for ISS Proximate Operations		Required docking sensors: 1. Trajectory Control Sensor (TCS) OR Hand-held LIDAR (HHL). 2. Centerline camera. 3. Payload Bay camera with range/range rate determination.	All required docking sensors are available.	Continue Final Approach and Docking	One or more required docking sensors are not available prior to docking.	If sensor may be regained, ABORT approach and initiate corridor backout. If all required sensors cannot be regained on RETRY, approach to dock may continue on a best effort basis.	
C2-105 B	Orbiter	ISS Proximate Operations	Shuttle Sensors Required for ISS Undocking		Required undocking sensor to measure ISS lateral displacement from Orbiter docking mechanism centerline.	Undocking sensor is capable of sensing 8º corridor.	Continue Undocking	Functional undocking sensor is not available.	ABORT undocking.	
C2-105 C	Orbiter	ISS Proximate Operations	Shuttle Sensors Required for ISS Flyaround Operations		Required flyaround sensors: Hand-held LIDAR (HHL).	Functional HHL is available.	Continue Flyaround. If HHL fails during flyaround, ABORT and perform BREAKOUT maneuver.	Functional HHL is not available.	ABORT flyaround.	

4 Critical Events at NASA Goddard Space Flight Center

4.1 GSFC Mission Design Practices

Goddard is involved in the design and operation of unmanned Earth science missions. "Rules for the Design, Development, Verification, and Operation of Flight Systems," *aka* the Gold Book, is GSFC's highest-level technical design standard for flight systems [9]. The GSFC systems engineering process explicitly covers telemetry for mission-critical events. The aim is to ensure that required telemetry is monitored during all mission-critical events to support anomaly investigations in the event of a mishap, so that future problems of a similar nature can be avoided.

The GSFC practices and procedures for incorporating critical events into mission design are as follows. At Mission Concept Review (MCR), mission-critical events are identified in the Concept of Operations. At Mission Definition Review (MDR), requirements for coverage of critical events are identified in ground system design. At Preliminary Design Review (PDR), operations for mission-critical events are addressed in the Mission Operations Concept and requirements for critical-event coverage are specified in the ground system design. Telemetry and command coverage of critical events is flowed down to the Operation Plan at Critical Design Review (CDR), and to the Operations Procedures at Operational Readiness Review (ORR). Finally, during mission operations checkout, the telemetry capability to support monitoring of critical events is verified.

In addition to design for critical-event monitoring, the Gold Book contains many lessons learned or rules of thumb for mission design. For instance, the Genesis mishap could have been prevented by Gold Book Rule 1.33: Polarity Checks of Critical Components, which states that "All hardware shall be verified by test or inspection of the proper polarity, orientation, and position of all components (sensors, switches, and mechanisms) for which these parameters affect performance." The rationale is that each spacecraft and instrument contains many components that can be reversed easily during installation. Unless close inspections are performed, and proper installations are verified by test, on-orbit failures can occur when these components are activated. This is precisely what happened on Genesis: The gravity switches to trigger deployment of the parachute were installed backwards and the spacecraft fell to its destruction.

The Mars Climate Orbiter (MCO) mishap is addressed by Gold Book Rule 1.12: Units of Measurement which states that "All design elements shall be specified and designed to ensure the consistent and compatible use of physical units of measure." The rationale is that critical functions can be misrepresented by errors in unit conversions. MCO missed orbital insertion around Mars, as an erroneous trajectory was computed using data in English units instead of metric units.

These particular mishaps could likely not have been prevented solely by critical event monitoring; once launched with gravity switches installed backwards, the Genesis mission was doomed (unless parachute deployment could be remotely commanded).

4.2 GSFC Operations Procedures

Goddard utilizes a combination of on-board fault protection and ground control to ensure spacecraft safety during operations. The spacecraft fault protection system is automated, as described in Appendix B – GSFC Automated Fault Protection. The spacecraft flight

software monitors key limits using a combination of Telemetry Statistical Monitors (TSMs) and Fault Detection and Correction (FDC) redlines, typically operating on single telemetry points. The TSM rules monitor the spacecraft at the system level, and are typically executed by Command and Data Handing (C&DH). The FDC rules are monitored for a particular subsystem only, and are executed within that subsystem. If a rule is triggered, indicating a violation of some safety or normal operations constraint, an automated recovery action may be initiated by a series of pre-programmed commands, the Relative Timed Sequence (RTS).

Ground control of spacecraft operations is semi-automated, using predefined procedures written in the Systems Test and Operations Language (STOL), and executed by the Advanced Spacecraft Integration and System Test (ASIST) ground command and control software at the Mission Operation Center (MOC). A suite of STOL procedures is developed to support operations for a mission. These procedures are sets of commands that can be issued by the MOC during a ground contact that the spacecraft will respond to. STOL procedures can include checks for required preconditions and expected responses, and as such implement GO/NO-GO checks on critical events in the system.

In general, the Goddard approach is to design out known anomalies as much as possible, and to respond to escapes through a combination of on-board fault protection, spacecraft safing, and ground-directed recovery. There are no critical events defined that require operator intervention within a specified time to ensure mission success. Recent efforts have been to increase automation and reduce the need for operator oversight, to reduce mission operations costs.

A few examples of critical events for remote sensing and earth science systems are:

- Science data collection and recording activities, instrument and sensor calibration
- Ground contacts to allow:
  - Uplink of commands to spacecraft, including absolute time command (ATC) loads and contingency operations
  - Science data downlink telemetry
  - Real-time and playback of state of health and satellite monitoring telemetry
- Station-keeping and orbital maneuvers
- Pointing accuracy for solar arrays (towards the Sun) and communication antennas (towards Earth).
- On-orbit separation and checkout, and deployment of the solar array

For satellite constellations, orbit formation operations are also critical events. For example, Earth Observing One (EO-1) is in polar orbit behind Landsat-7 (L7) by one minute. Weekly orbital maneuvers must be performed in order to maintain the L7 co-fly profile. This facilitates co-imaging activities and prevents collision between the satellites.

4.3 GSFC Critical Events for Earth Sensing Satellites

Critical events for earth observing missions are analyzed in Table 3. These critical events are based on contingencies for the Earth Observing One (EO-1) satellite.

Table 3: GSFC Remote Sensing Satellite Critical Events and Corresponding GO/NO-GO Determinants

Mission Phase	Critical Event	Subsystem	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomalous Pre-Commit (NO-GO)	Anomalous (NO-GO) Recovery	Subsystem Interactions (Y/N)
On-orbit	Science data collection	Science Instruments	TSM 017: Get direction of Sun from Coarse Sun Sensor (CSS) Spacecraft Z axis	Instruments pointing away from the sun.	Instruments pointing away from the sun.	TSM 067: Instruments pointing toward the sun.	TSM 067 action: If Z Axis within 30 degrees of the sun then go to safemode.	Y
On-orbit	Science recording	Science Recorder	Wideband Advanced Recorder Processor (WARP) Reset Count	WARP recording, no reset.	WARP data recording complete. No resets.	TSM 074: WARP Reset	TSM 074 action: WARP experienced a reset during memory operation. Turn WARP off (RTS 21)	N
On-orbit	Instrument and sensor calibration	Science Instruments	Advanced Land Imager (ALI) focal plane temperature	ALI Focal Plane temperature within nominal operating range	ALI and Hyperion temperatures within normal operating ranges. No instrument resets.	TSM 116: ALI Focal Plane Too Cold	TSM 116 action: If ALI focal plane < -83ºC then execute RTS 61 to turn on the outgas heater	N
			ALI Control Electronics (ALICE) Radiator Temperature	ALICE temperature within nominal operating range		TSM 100: Excessive ALICE Temperature	TSM 100 action: If IHSKP_T36 is 59ºC, then call RTS 8	
			ALI Focal Plane Electronics (FPE) Temperature	ALI FPE temperature within nominal operating range		TSM 101: Excessive FPE Board 1 Temperature	TSM 101 action: If IHSKP_T36 > 50ºC, then call RTS 8	
			Hyperion Visible Near Infrared (VNIR) Analog Signal Processor (ASP) Temperature	Hyperion VNIR ASP Temperature within nominal operating range		TSM 152: Hyperion VNIR ASP (external) too hot	TSM 152 action: If Ext temp > 55ºC for > 3 telemetry packets, then shutdown Hyperion (RTS 28)	
			Hyperion Short Wave Infrared (SWIR) Analog Signal Processor (ASP) Temperature	Hyperion SWIR ASP temperature within nominal operating range		TSM 153: Hyperion SWIR ASP (external) too hot	TSM 153 action: If Ext temp > 55ºC for > 3 packets, then shutdown Hyperion (RTS 28)	
			Hyperion Reset watchdog timer (YWDOGRST)	No Hyperion reset.		TSM 160: Hyperion Reset Watchdog Timer	TSM 160 action: Hyperion Reset (RTS 38) if watchdog timer reset bit == 1	
Contact	Establish communication link and send packets	Attitude Control Subsystem (ACS), Communication C&DH Power, Science Recorder	TSM 022: Attitude Control Electronics (ACE) Housekeeping (HK) Telemetry TSM 023: Power System Electronics (PSE) Fast Telemetry TSM 024: COMM HK Telemetry TSM 028: CI Codeblock Counter Attitude sensors: 3-axis Magnetometer (TAM), Inertial Reference Unit (IRU), Autonomous Star Tracker (AST).	Acquisition of Signal (AOS). Attitude sensors indicate antenna pointing accuracy to ground station. Ground uplink of commands to spacecraft: Absolute time command (ATC) loads and contingencies. X-Band downlink of real-time/playback science data. S-Band State Of Health and satellite monitoring telemetry.	Loss of Signal (LOS) after transmission complete.	TSM 233: X-Band Phase Array Too Hot	TSM 233 action: If > 65ºC for > 10 seconds, then turn off XBand (RTS 6)	Y
						TSM 215: ACE Remote Service Node (RSN) Errors and Losing Power	TSM 215 action: No ACE telemetry for > 20 min and BSOC < 80% and Battery voltage < 26.3V, then Power Cycle the ACE (RTS 11)	
						TSM 216: PSE RSN Errors	TSM 216 action: If no PSE telemetry for > 1 minute, then send warm boot command (RTS 11)	
						TSM 232: No Codeblocks received for 5 days	TSM 232 action: If no command (codeblock) received for 5 days then, attempt downlink (RTS 27)	

Mission Phase	Critical Event	Subsystem	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomalous Pre-Commit (NO-GO)	Anomalous (NO-GO) Recovery	Subsystem Interactions (Y/N)
On-orbit	Power Management	Solar Array Power ACS	TSM 011: Get Battery Current TSM 016: Get battery end-of-night voltage Battery State Of Charge (SOC) Battery Voltage Battery Temperature TSM 017: Get direction of Sun TSM 022: ACE HK Telemetry TSM 023: PSE Telemetry Attitude sensors: 3-axis Magnetometer (TAM), Inertial Reference Unit (IRU), Autonomous Star Tracker (AST).	TSM 030: HOP 1 Power TSM 031: HOP 2 Power TSM 056: S/A Disabled Attitude sensors indicate pointing accuracy for solar arrays perpendicular to sun.	TSM 056 action: If the S/A is disabled, then enable it.	TSM 050: Low Battery State Of Charge (SOC)	TSM 050 action: If > 30% and < 70% call Safe Power RTS #19. If < 85% issue event message	Y
						TSM 053: Battery SOC < 90% at End Of Day	TSM 053: Issue event message	
						TSM 054: Half Battery Voltage Differential	TSM 054 action: If > 0.35V, then RTS 19 If > 0.08, then event message	
						TSM 055: Battery Temperature high	TSM 055 action: If > 25 deg, call RTS 18 If > 23 deg, issue event message	
						TSM 060: Battery Voltage Too Low	TSM 060 action: If Bat V < 26.3, then RTS 59. If < 26.8, then event message	
						TSM 065: Solar Array too hot	TSM 065 action: If > 50ºC for 3 samples, then event message	
						TSM 076: Chassis Current Too High	TSM 076 action: If chassis current > 1 Amp, then loadshed. If chassis current > 0.2 Amp, then event message	
						TSM 103: Out of Range ALICE 28V Current	TSM 103 action: If IHSKP_SPEP28V > 2.5 Amps then call RTS 7 (shutdown)	
						TSM 207: AC Power Supply Board (PSB) Too Hot	TSM 207 action: If AC PSB temp > 328ºK for 4 samples, then turn off AC (RTS 20)	
Checkout	Separate and Deploy Solar Array	Solar Array Power	TSM 007: Separation Signal 1 TSM 008: Separation Signal 2 TSM 009: Separation Signal 3 TSM 018: Get S/A Yoke Deployment TSM 019: Get S/A 1st Panel Deployment TSM 020: Get S/A 2nd Panel Deployment TSM 021: Get S/A 3rd Panel Deployment	TSM 063: Pre-Sep Power-On Powered on with at least two signals showing attachment to the Launch Vehicle.	TSM 063 action: Prepare for separation (RTS 36)			Y
				TSM 073: S/A Deployed All four signals (TSMs 18, 19, 20, 21) indicate full deployment (> 95%).	TSM 073 action: Begin deployment sequence (RTS 35)			
				TSM 075: (HOP)s on and S/A Deployed Either HOP LVPC service is on and any two S/A potentiometers show release (20%).	TSM 075 action: Turn off HOPs (RTS 60)			

Mission Phase	Critical Event	Subsystem	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomalous Pre-Commit (NO-GO)	Anomalous (NO-GO) Recovery	Subsystem Interactions (Y/N)
On-orbit	Orbital Maneuvers	ACS Power	Delta-v Attitude sensors: 3-axis Magnetometer (TAM), Inertial Reference Unit (IRU), Autonomous Star Tracker (AST). Available propellant Range/velocity wrt constellation members	Station Keeping Sufficient propellant must be available for deorbit burn. For Formation Flying, at least 1 minute separation.	Station keeping with required propellant and separation margins.	TSM 066: Detect ACE in Safehold	TSM 066 action: If ACE is in safemode, configure the spacecraft for safemode (RTS 2)	Y
						TSM 068/069/070: High Rotation Rate	TSM 068/069/070 actions: If Gyro rate in any axis > 1 deg/sec, then close latch valve (RTS 4)	
						TSM 234: Thrusters on too long	TSM 234 action: If thrusters on for > 24 sec, then turn thrusters off (RTS 26)	

5 Critical Events at NASA Jet Propulsion Laboratory

5.1 JPL Mission Design Practices

JPL-specific standards for flight systems that address critical events are the "JPL Flight Project Practices" [7] and the "JPL Design, Verification/Validation and Operations Principles for Flight Systems" [8]. Other related documents are JPL Standard for Systems Safety [12], JPL Anomaly Resolution [13], and JPL Reliability Assurance [14].

JPL defines mission-critical events as those that if not executed properly, could result in failure to achieve mission success (e.g., orbit insertion, EDL). Fault tolerance design principles include sequence continuation in response to non-survival-threatening anomalies; safing in response to survival-threatening anomalies, requiring ground intervention for recovery; on-board backup sequence execution in the event that command upload capability is lost; and ample diagnostic engineering telemetry, including telemetry data downlinked for critical events.

Prior to launch, projects develop the flight sequences for launch and early flight operations, and develop a baseline version of mission-critical sequences (orbit insertion, entry/descent/landing, launch and launch vehicle separation, deployments, etc.) and mission-enabling sequences (science operations, aero braking, safing, etc.). JPL defines a series of documents that address sequences for mission-critical events, including Sequence Activity Plans, Spacecraft Anomaly Recovery Plans, Contingency Plans, and Flight Rules and Constraints. These are defined specifically for each mission.

Flight sequence design for critical sequences ensures telemetry visibility for real-time monitoring and verification of mission-critical events. This requires sufficient telemetry data to rapidly assess spacecraft state and health status under normal and faulted operations, so that ground operators can determine rapidly and unambiguously the state of the spacecraft early in the ground tracking pass, including whether the spacecraft executed a fault protection response. Adequate telemetry data and sampling frequency, including any special diagnostics, are required to enable the flight team to perform anomaly determination, investigation, and reconstruction.

Mission design provides for redundant handling of mission-critical sequence data with simultaneous real-time transmission and on-board storage. On-board storage protects critical data against loss in the event of selected anomalies, (e.g., transient power or communications outage). The design also includes the design of fallback or contingency options that specify how the mission will adapt to failures or performance shortfalls in mission-critical systems. Missions with single-string design for critical events may need to increase functional redundancy or control algorithm robustness. Single-string design is acceptable if the demonstrable risk is acceptable.

Mission assurance practices include Hazard Analyses, which identify and assess hazards associated with the design and operation of flight hardware and mission-critical software. Initial analyses are performed as early as practical in the formulation phase and are updated as needed through launch. For hardware, single points of failure that are part of success-critical functions are identified by Failure Modes, Effects, and Criticality Analysis (FMECA) for electrical/electronic hardware, or by a Fault Tree Analysis for devices, mechanisms, and electro-mechanical hardware. Risk assessments evaluate the measures implemented to minimize risk, including alternate operating modes, operational

workarounds, and telemetry sources of failure information. Single points of failure are eliminated from the design where possible, or a waiver is requested.

Software quality assurance includes verification of the software traceability matrix to ensure that requirements are correctly implemented and that critical mission software has been appropriately tested. For safety/mission-critical flight software with a significant risk, the NASA Independent Verification and Validation (IV&V) Facility is used.

The mission team performs system-level functional V&V of the launch sequence and early flight operations on the flight vehicle, using the launch version of flight software. Commands and sequences for all critical events are developed, tested, and verified prior to launch. This includes validation of baseline versions of mission-critical sequences and mission-enabling sequences. Verification is by functional simulation, and includes checks of flight rules and resource utilization constraints (e.g., power, data rate, thermal conditions).

5.2 JPL Operations Procedures

Mission operations practices are documented in the "JPL Flight Project Practices" [7]. Operations teams give special attention to checkout of flight system functionality, and the development of sequences for mission-critical events, especially for irreversible events. Critical Event Readiness Reviews (CERRs) are conducted sufficiently in advance of critical events to allow time for correction of deficiencies. Prior to irreversible events, the operations team assures safe, reliable operation in the design of sequences, for instance by reviewing relevant development history including red-flag PFRs (problem/failure reports). Prior to mission-critical events, the operations team identifies what could go wrong (e.g., using an event fault tree) and develops contingency plans to ensure that each critical event occurs. When a time-critical response is required, contingency surface operations procedures and sequences are generated and validated to the level needed to facilitate a rapid response.

The readiness of the operations team for upcoming critical events is demonstrated for both nominal and off-nominal conditions by Operations Readiness Tests (ORTs). Prior to uplink of the critical event sequence, the sequence is validated by testing nominal and off-nominal execution on the Flight System Testbed, by internal review of the sequence and by external walkthrough of the sequence and review of the testbed test results. The operations team manager approves the critical event sequences, as well as any waivers to flight rules that may be necessary.

The command load for the next day's activities is generated during each nighttime period for the spacecraft, validated, and then uploaded to the spacecraft. Prior to command load execution, successful upload of the sequence is verified, for instance by checking the on-board memory for corruption that could result from single-event upsets, using checksum telemetry.

All sequences should execute pre-stored, pre-validated Relative Time Sequences (RTSs) for standard kinds of regularly used functions where available, instead of including new commands for those functions in the new sequence. Relative or event-driven sequences are pre-stored for foreseeable repeating functions, to be available for reuse in new sequences without requiring re-validation. At a minimum, non-standard portions of sequences that have not previously been validated shall be simulated on the testbed prior to being uplinked to the spacecraft. A portion of the sequence is non-

standard if it contains a single command not normally belonging to the standard sequence, or if it has not been tested previously on the testbed.

5.3 JPL Critical Events for the Mars Exploration Rovers

Critical events for rover surface operations for the JPL Mars Exploration Rover (MER) program are analyzed in Table 4. MER critical events are based on constraints listed in Appendix C – JPL Mars Exploration Rover Flight Rules, as well as an extensive spreadsheet of MER flight rules that is too lengthy for inclusion in this report. Additional critical event information has been taken from the JPL CLARAty project. CLARAty (Coupled Layered Architecture for Robotic Autonomy) is a robotic architecture that is being used to mature and validate technology for infusion into future JPL rover missions.

Some acronyms used in the table are:

Absolute Time Command (ATC)
Acquisition of Signal (AOS)
Alpha-Particle X-ray Spectrometer (APXS)
Battery State of Charge (BSOC)
Charged Coupled Device (CCD)
Command and Data Handling (C&DH)
Deep Space Network (DSN)
Flight Software (FSW)
High Gain Antenna (HGA)
Inertial Measurement Unit (IMU)
Instrument Arm (IA)
Instrument Deployment Device (IDD)
Loss of Signal (LOS)
Microscopic Imager (MI)
Mini-Thermal Emission Spectrometer (Mini-TES)
Mission Clock (MC)
Mission Elapsed Time (MET)
Mossbauer spectrometer (MB)
Quaternion (rover position estimate)
Rock Abrasion Tool (RAT)
Solar Array (SA)
State of Health (SOH)
Universal Coordinated Time (UTC)
Visual Odometry (VO)

Table 4: JPL Rover Critical Events for Surface Operations

Reference Number	Critical Event	Subsystems	Measurement/Telemetry	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomaly	Recovery
#1 (CLARAty)	Traverse Over Challenging Terrain	Mobility Navigation: IMU Odometry VO Sun Sensor	Wheel 1 Motor Encoder Wheel 2 Motor Encoder Wheel 3 Motor Encoder Wheel 4 Motor Encoder Wheel 5 Motor Encoder Wheel 6 Motor Encoder Steering 1 Motor Encoder Steering 2 Motor Encoder Steering 3 Motor Encoder Steering 4 Motor Encoder Steering 5 Motor Encoder Steering 6 Motor Encoder Suspension angles: - Left Rocker-Bogie - Right Rocker-Bogie - Rocker Pot Pose estimate: - Rover Local Position X - Rover Local Position Y - Rover Local Position Z - Rover Heading (yaw) - Rover Tilt (pitch) - Rover Roll Rover acceleration/ rotation/velocity (IMU): - xyz angular gyroscopes - xyz accelerometers Pose estimate covariances: - VO covariance - Sun Sensor covariance Time	Status nominal for all: - Wheel motors and encoders - Steering motors and encoders - Rocker-bogie suspension - IMU, Odometry, VO, and Sun Sensor. Daytime. Don't drive after dark or before 08:10 (see rule on warmup). Terrain is safe. Nominal Pose Estimation: Pose estimation localization error is small. All sensors in close agreement. Utilizes Kalman filter to weight sensor inputs from IMU, Odometry, VO, and sun sensor, based on covariance matrix. VO and sun sensor supply covariance data, IMU and odometry covariances are fixed. Localization error is overall covariance, calculated by Kalman filter based on individual sensor covariances. Nominal Sun Sensing: Takes picture of sun at specific time, detects sun based on grayscale levels. Uses almanac to predict where sun should be, from this computes Rover Heading relative to true north. Nominal Visual Odometry: Stereo pair camera takes images, computes rover motion from images. Nominal Odometry: Encoders in the wheels, count as wheel rotates.	Rover progress, according to pose estimation, is as expected. Continue traversing.	Mechanical failure: 1. Wheel/steering motor locked 2. Wheel/steering motor stalled 3. Wheel/steering motor spins free 4. Wheel/steering encoder fails (noisy/garbage, stale or no data) 5. Suspension failure (not likely) Rover progress is less than expected.	Other wheels compensate for failed wheel. Drive backwards to nurse a gimpy front wheel.
						Terrain too hazardous. Rover progress is less than expected. 1. Stalling of multiple wheel motors 2. Overheating of multiple wheel motors 3. Extreme rocker-bogie suspension angles 4. Hanging wheel/drop-off indicated by negative rocker-bogie angle 5. Wheel slippage, lack of traction (too steep/soft sand) If wheels slipping, Kalman filter detects Odometry diverges from other sensors' pose estimate. Large covariance.	ABORT traverse.
						Sun sensor failures: 1. Camera fails. No image. 2. Sun occluded by object (by terrain/mast, sunrise/sunset/dust-storm). 3. Camera covered by dust. With dust accumulation, covariance estimate grows over time. Error indicated by large covariance.	Pose estimation covariance exceeds maximum tolerance. Kalman filter combines results only from good sensors. Compensates for VO and sun sensor failures only, which have covariance inputs.
						IMU fails: 1. Noisy or garbage data 2. No data 3. Stale data	
						VO failures: 1. Stereo pair camera fails 2. No detectable features in image, to detect motion. If no features, covariance is large.	

Reference Number	Critical Event	Subsystems	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomaly	Recovery
#2 (CLARAty)	Imaging for Situation Assessment And Science	Stereo Hazcam / NavCam / PanCam	Camera state Framegrabber error codes. Image state: Exposure Gain Brightness Iris Focus Dynamic range (balances white and black pixel count in the image). Quaternion.	Camera state nominal. Image parameters in nominal ranges. Rover is stationary for science images.	Image state nominal. No deleterious image effects - e.g., dynamic range not exceeded.	Camera failures: 1. Framegrabber failure (analog) 2. CCD failure (digital) 3. All pixels are black in an image Image failure effects: 1. Over-exposure 2. Under-exposure 3. Dynamic range exceeded if very high contrast 4. High-gain noise for dark images 5. Dust on lens 6. Fixed-pattern noise 7. Blooming 8. Gaps in image	For camera failure, switch to other available cameras. For over-exposure, decrease exposure time/gain. For under-exposure, increase exposure time/gain. Tradeoff is that gain also increases noise. Reframe image to reduce dynamic range - e.g., no sky.
			Stereo Disparity Density: measures percentage of pixels that successfully overlap in the stereo image pair.	For stereo cameras, pixels in left camera *must* have fixed relationship to right camera and rover body. For analog cameras, synchronization signal is connected to both cameras to initiate exposure at same time.	Stereo cameras correctly aligned. Cameras exposed at the same time. Recognizable pixels exist to calculate disparity density. Image pair state nominal.	Stereo co-imaging failures: 1. Cross-eye (camera orientation calibration error) 2. Lack of sync between left and right cameras 3. Lack of features to calculate disparity density - e.g., plain sand, blank sky	Lack of sync between left and right cameras plus rover motion or mast vibration causes low disparity density. Lack of sync may be tolerated if rover and mast are completely still. If rover state indicates possible motion influencing image, retake image when still.
#3 (MER Flight Rule)	Downlink Science, Uplink Command Loads	Comms HGA Science Recorder C&DH Avionics and Sequencing	HGA state Signal state (AOS/LOS) Science data SOH Rover telemetry Science Recorder state ATC loads Contingency operations Command Loss monitor UTC	AOS. Playback and transmit science/SOH from Science Recorder. Transmit real-time SOH/telemetry data. Verify sufficient on-board data storage for recording command loads. Need a minimum of ten days of surface operations commands; thirty days of contingency action commands; current daily commands. Uplink ATC/contingency command loads to rover. Clock drift must be accurately accounted for when uploading sequence commands. Time Correlation (TC) packets are downlinked periodically through out all phases of the mission, and more frequently during surface operations, when clock drift is worst.	Successful playback of Science Recorder data. All science/SOH telemetry packets successfully transmitted. Command upload verified. To ensure commands are properly received, ATC loads/critical commands are only transmitted if DSN tracking coverage and rover state allow verification. LOS	Failure to acquire signal. Failure to transmit science/SOH telemetry data. Science Recorder fails to playback science/SOH data. Failure to empty Science Recorder after playback. Failure to receive new rover command sequence or to verify command load. Command Loss monitor detects loss of uplink. Command load time changes from relative to absolute time result in a time less than current mission clock (clock drift). All commands whose time has already passed will execute immediately.	If an uplink acquisition is missed during the normal uplink period, repeated uplink attempts shall be initiated prior to the normal sequence activation time. If command uplink not successful prior to the nominal activation time, special action to maintain flight system safety must be considered.

Reference Number	Critical Event	Subsystems	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomaly	Recovery
#4 (CLARAty)	Instrument Placement and Sampling	IA Science Instruments Science Recorder	IA Joint 1 Angle IA Joint 2 Angle IA Joint 3 Angle IA Joint 4 Angle Instrument state Instrument-specific calibration parameters. Science Recorder state Available storage. Maximum storage capacity.	IA, instrument, Science Recorder states nominal. Arm joints are commanded to: unstow/extend/ retract/grasp/contact/stow/change tool. Turn wheels out of IA workspace for imaging/science operations. Verify sufficient on-board data storage for recording science.	IA successfully executes command. Instrument successfully samples or collects data, and Science Recorder records data.	IA failure to unstow/extend/retract/ grasp/contact/stow/change tool. 1. Single IA Joint fails. 2. Single IA Encoder fails. 3. Multiple IA joints/encoders fail. Instrument error/calibration error. Science Recorder fails to record data collected by instrument or Science Recorder file system corrupted.	If one joint fails, reconfiguration with remaining degrees of freedom in the arm to achieve desired position may be possible. If Science Recorder full, delete old files.
#5 (MER Flight Rule)	Power Management	Power Solar Arrays	BSOC SA state MET	BSOC nominal. SA state nominal. Prior to day 30 on the surface, the minimum BSOC is ≥ 40%, thereafter it is ≥ 20% (accounting for uncertainty in the environmental effects of dust deposition and dust in the atmosphere)	BSOC nominal SA state nominal	Battery cell voltage drops below minimum (3.2 V). Battery overheats. SA fails to provide nominal charging current. SA fails to deploy. Mission clock power loss and subsequent cold reboot. On MC power loss, spacecraft time is lost, defaulting to 01 January 2007 12:00:00, killing all sequences. The MC is powered ON through out all phases of the mission until batteries are no longer capable of sustaining Avionics overnight.	For low BSOC, battery discharge relay is opened to load shed all except the MC power. This is a serious fault which subjects the rover to potential loss of thermal control. The ground should be in the loop for any time recovery scenarios. To set the spacecraft time, ground issues the command ADJUST_TIME / SET_SC_CLOCK.
#6 (MER Flight Rule)	Thermal Regulation of Mechanisms, Instruments	Thermal, Mechanisms, Science Instruments	Commandable heaters: parameter designating heater(s). Heater switch states. Temperature sensors. Warmup heaters for: Mobility, IDD/IA, SA, HGA actuator motor and gearbox, PanCams, HazCams, NavCams, MI and dust cover, camera azimuth/elevation actuators, and filter wheels. Time of day.	Check time of operation and ambient temperature. Check time intervals for operation of device within specification. If late in the day and warm enough, nominal operation may be possible without warmup. If not too early/ cold, warmup actuators/instrument to -55°C to ensure operation of device within specification. For mobility, if a drive command is detected, ensure warmup heaters are turned on.	Mechanism/ instrument warmed-up to within operating temperature range specification.	Operation earlier than allowed time for the device. Size of heater and ambient environment prevent device from being warmed to -55°C. Heater or switch failure prevents warmup. Temperature sensor failure prevents accurate thermal control. Instrument temperature regulation failure: overheating, freezing. Some instruments e.g. Mini-TES can be damaged by cold.	If no warmup of mobility actuators, motors will operate more slowly, with no h/w damage.
#7 (MER Flight Rule)	Prevention of Dust Contamination / Interference of concurrent rover activities	RAT, Science Instruments	RAT state Science instrument states: PanCam, MI, MB, Mini-TES, APXS	No use of science instruments (PanCam, MI, MB, Mini-TES, APXS) during RAT operations. Science instruments stowed and/or dust covers in place.	Dust-sensitive instruments protected from RAT-generated dust. Power usage during RAT activities is minimized.	RAT operations occur during science data collect or with instrument dust covers open. Instruments contaminated by dust, with resulting performance degradation.	Abort RAT operation.

Reference Number	Critical Event	Subsystems	Measurement	Nominal Pre-Commit (GO)	Nominal Post-Commit (GO)	Anomaly	Recovery
#8 (MER Flight Rule)	Prevention of Dust Contamination	Science Instruments	PanCam state PanCam azimuth/elevation MI state MI cover state MI azimuth/elevation	When not operating, the Pancam cameras are stowed to prevent the accumulation of settling atmospheric dust particles on the optics. The MI dust cover shall be open only during MI imaging: opened just before imaging, and closed immediately after imaging. At no time shall the MI be positioned such that its boresight is oriented above the nominally horizontal plane and its dust cover is open (while in position to image natural surface).	Minimizes dust buildup on the PanCam/MI optical surfaces.	PanCam not in stowed position when not in use. Stowed position is at elevation angle of -90 degrees. Dust accumulation degrades the radiometric calibration of the PanCam cameras. Understanding of the PanCam's wavelength response is permanently compromised, and stray light increased by an unknown amount. MI dust cover state not closed when not in use. Dust accumulation on the MI optics degrades performance of the instrument.	
#9 (MER Flight Rule)	Interference between concurrent rover activities	Mobility/ Navigation IDD HGA Science Instruments	Quaternion. IDD state HGA state Science instrument states: PanCam, MI, MB, Mini-TES, APXS Hazard map	Constraints on simultaneous science data collect/rover traverse/ IDD actuation/HGA actuation activities. During science operations, no movement of rover or IDD/HGA activity. Specifically, no motion of wheels, steering motors or actuators while PanCam, MI, MB, Mini-TES, or APXS are acquiring data. Includes no IDD or HGA actuations during PanCam, MB, or Mini-TES data collect; and no motion of the rover or any mechanical device during sungaze. During driving, rover motion shall not endanger IDD. The IDD shall be in a stowed position whenever rover wheels or steering motors are actuated. No camera activities concurrent with rover orientation determination/pose estimation update.	Successful science data collect or rover traverse or IDD actuation or HGA actuation. After any rover driving, the IDD shall not be moved until the flight team has verified that it has adequate clearance for its next move, taking into account uncertainty in the post-move location of the rover.	Science compromised by movement of rover or IDD/HGA actuation during science operations. Actuation/movement during imaging causes image blur/ smearing; or degradation of spectra acquired. Possible damage to IDD and/or instruments by contact with terrain when driving, if IDD not stowed. IDD/HGA movement causes microphonics interference (vibration noise) that degrades MB spectral acquisition and Mini-TES interferometery. UPDATE_ATTITUDE during imaging causes panoramic mosaics to be improperly stitched, as if the rover were in two different positions.	Abort drive/IDD actuation/HGA actuation/data collect. Retry only one. Stow IDD before drive.

6 Summary and Recommendations for Future Work

The general approach taken to reduce risk of a mission is to design out credible single faults where possible; mitigate risk using redundancy in design; plan for residual risk through operations procedures and contingencies; and accept risk through waivers. Since mission success requires the successful execution of critical events, and failures involving critical system functions can lead to mishap, critical events must be understood as a key component of risk analysis.

This report investigates how selected NASA centers deal with critical events as a matter of mission design and operations. State of the practice in mission design processes and operations procedures for critical events was surveyed, as well as major critical events for active missions at three NASA centers: ISS at JSC, EO-1 at GSFC, and MER at JPL.

For these sample missions, specific critical events and their attributes were identified from analysis of GO/NO-GO flight procedures, on-board automated fault protection, and flight rules. Analysis was conducted on a case-by-case basis, and each critical event was defined in terms of GO/NO-GO decisions made under nominal and anomalous scenarios. The information gathered by this approach is very domain specific. Since there is little in common between the ISS, EO-1, and MER missions, their critical events show little overlap. However in a larger sampling of missions with similar mission phases, it is expected that critical events will show commonality at the appropriate level of abstraction. This will more readily allow comparison of critical events across missions and mishaps, to identify recurrent themes and discern trends.

It is therefore recommended that a larger survey be undertaken in order to identify classes of critical events and attributes that are not adapted to a specific mission. This survey was just a small beginning in this process. It is also recommended that a more systematic method be developed for identification and analysis of critical events across missions and mishaps; this could be a classification method, taxonomy, or set of guidelines. For instance, any activity involving a shared resource where unavailability of that resource impacts mission goals, such as a solid state recorder or downlink communications, has the potential for resource conflict and over-subscription. As a guideline, this helps to identify such activities as candidate critical events.

Examination of the procedures at the three NASA centers indicated that processes appear to be tailored to the particular applications and needs of the center. There is little reuse of the body of knowledge across the agency to take advantage of overlap and commonality where it does exist. A long-term goal for further work would be to ensure that standard practices, design guidelines, techniques, and operating procedures for critical events are developed.

Short-term steps could be to send a questionnaire out to participating centers (JSC, GSFC, and JPL), to assess more fully their practices for handling of critical events, and to engage the centers in the assessment. The survey could include questions that help determine whether a critical event is a hard or soft critical event, mission critical or mission enabling, and whether sufficient data is monitored at the pre-commit to ensure coverage of the critical event. Additional work could be to flow-chart the process at each center, following a critical event and tracing it through the design process, operations

procedures, and anomaly resolution procedures. The charts from each center could then be compared to seek a basis for standardization.

7 Conclusions on the Role of Critical Events in Design and Operations

Although this report targeted active missions, critical events may also be analyzed early in the mission concept phase, even before traditional methods such as an integrated risk assessment (IRA) are applicable. This is due to the fact that the critical event can be meaningfully expressed at a higher level of abstraction. An IRA focuses on hazards or failure modes for each component, with cause and effect, criticality, and corrective action, and requires design to be far enough advanced for component selection to have been made. The scope of critical event analysis is also wider than that of an IRA, as both nominal and anomalous operations are examined.

The importance of early analysis of critical events and its link to operations has further implications. Long-term operations costs and risks in the ISS program were impacted by lack of systems integration between flight/ground design and operations, and lack of involvement of operations in early design [15]. The concept of the critical event permeates the system life cycle, the thread running through system specification to the implementing operations procedures and flight rules that monitor and verify that critical events take place as planned. Traditional systems engineering processes may be used to define system functional requirements for critical events, as well as for verification and validation of coverage and traceability of critical events from mission design through operations. Operators and designers equally understand the importance of critical events; critical events may provide the common ground to better link the design phase to mission operations, and ensure that operations needs are taken into consideration early in the design.

Critical event analysis reduces risk by providing guidance to designers, operators, and program managers as to the requirements for sensing, monitoring, telemetry, and data collection, to help ensure that adequate observation and decision-making capabilities are in place during mission-critical events. There is a natural tension between engineering staff who want more data and systems for improved reliability and performance, and program managers who want to limit cost and schedule. As an example, in order to manage the Mars Polar Lander program within the established cost constraints, the decision was made not to expend any resources on efforts that did not directly contribute to landing safely on the surface of Mars. On that basis, no telemetry was provided for Entry, Descent, and Landing. As a result, the MPL mishap occurred in a telemetry blackout, and the incident had to be painfully reconstructed without data from the spacecraft.

An understanding of critical events may help prioritize mission design and operations decisions that trade off cost and schedule against risk and technical resources. This prioritization assists in the optimal allocation of limited resources and establishing safe margins for critical performance parameters such as mass, power, propellant, telemetry bandwidth, CPU speed, control cycle rates, interrupt rates and durations, memory and cache sizes, etc.

Trends suggesting that unintentional subsystem interactions have become a significant cause of mishaps since 1997 have been identified [11]. The potential for mishaps involving subsystem interactions is supported by the small sampling in this

report; all of the identified critical events for JSC's rendezvous and docking involve interactions of multiple subsystems, of the Shuttle and Station systems. For GSFC, many of the identified critical events cross subsystem boundaries, as indicated in Table 3. For JPL rovers, critical events cross subsystem boundaries in most cases. Critical events provide a means of analyzing subsystem interactions and generating or validating subsystem interface requirements, such as expected subsystem interface parameter values under various critical operating conditions (e.g., GO/NO-GO, nominal/anomalous). This has greatest impact during early design, and results may later be flowed down to detailed subsystem interface control documents.

The long-term vision for mission operations includes autonomous operations and health management of critical events. Remote missions would benefit most from autonomous health management of critical events, for local oversight when it is needed most. Mission operations can be conducted by JSC in real time, since Shuttle and Station are in low-earth orbit and communications delays are on the order of seconds or less. JPL must pre-plan and carefully verify command sequences before upload, as the 20-minute Mars communication delay precludes real-time remote mission operations. GSFC operations are the least constrained, in that critical events are not human rated and do not have significant communication delays in Earth orbit. As this environment is relatively low risk, GSFC may be open to autonomous critical events, as is currently demonstrated by the Autonomous Sciencecraft Experiment (ASE)/Livingstone 2 software that is autonomously monitoring and operating EO-1 [16, 17]. Once autonomous operations are proven for critical events in low-earth orbit on an unmanned spacecraft, this can be extended to critical events for more challenging and remote missions.

8 Acknowledgements

The following people were helpful contacts for this survey. Special thanks to Tina Panontin, Alan Crocker, Dan Duncavage, Carol Russo, Kanna Rajan, Seth Shulman, and Tracy Neilson.

JSC:
Ernest Smith
Alan R. Crocker
Dan Duncavage
Bruce Hilty
Steve Gonzalez

Ames:
Tina Panontin (Ames Chief Engineer)
Carol Russo
Kanna Rajan (for MER information)
Roxana Wales

GSFC:
Dan Mandl (EO-1 Flight Director)
Stu Frye
Seth Shulman

JPL:
Tracy Neilson

9 References

1. The Diaz Report, "An Assessment of the NASA Agency-Wide Applicability of the Columbia Accident Investigation Board Report," January 30, 2004.
2. The CAIB Report, "Columbia Accident Investigation Board Report," August 2003.
3. JPL Special Review Board, "Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions," JPL D-18709, 22 March 2000.
4. "Mars Climate Orbiter Mishap Investigation Board Phase I Report," November 10, 1999.
5. JPL Special Review Board, "Mars Observer Loss of Signal: Special Review Board Final Report," JPL Publication 93-28, November 1993.
6. "CONTOUR Comet Nucleus Tour Mishap Investigation Board Report," May 31, 2003.
7. Jet Propulsion Laboratory, "Flight Project Practices," DocID 58032, Rev 5. Feb 27, 2003. (http://standards.jpl.nasa.gov/contractor/docs/dmie58032-5.html)
8. Jet Propulsion Laboratory, "Design, Verification/Validation, and Operations Principles for Flight Systems (D-17868)," Revision 2, March 2003. (http://standards.jpl.nasa.gov/contractor/docs/d17868-2.html)
9. Goddard Space Flight Center, "Rules for the Design, Development, Verification, and Operation of Flight Systems (GSFC – STD – 1000)," *aka* "The Gold Book", Baseline Release, December 10, 2004.
10. Earth Observing-1 Contingency Document Section 4: EO1 Power Balance Contingencies.
11. Dr. Tina L. Panontin and Dr. David Bell, "Mishap Cause Classification Study," 2002.
12. JPL Standard for Systems Safety, D-560, March 1999. (http://standards.jpl.nasa.gov/contractor/docs)
13. JPL Anomaly Resolution, D-8091, May 2005.
14. JPL Reliability Assurance, D-8671, November 2001.
15. Ted Kenny and Jim Carr, "Techniques and Strategies for Reducing Long-Term Operations Cost/Risk During Early Vehicle Design," Mission Operations Directorate, NASA JSC, May 2004.
16. S. Hayden, A. Sweet, S. Christa, D. Tran, and S. Shulman. "Advanced Diagnostic System on Earth Observing One". *Proceedings of AIAA Space 2004 Conference and Exhibit, San Diego, California, Sep. 28-30, 2004.*
17. S. Hayden, A. Sweet, and S. Shulman. "Lessons Learned in the Livingstone 2 on Earth Observing One Flight Experiment". *Proceedings of AIAA Infotech@Aerospace 2005 Forum, Arlington, Virginia, September 2005*.
18. John Hopkins University Applied Physics Laboratory, "The NEAR Rendezvous Burn Anomaly of December 1998," November 1999.
19. "Report of the Presidential Commission on the Space Shuttle Challenger Accident", *aka* the Rogers Commission Report, June 1986.
20. Goddard Space Flight Center, "EO-1 Contingencies Document, Version 6.0," April 2003.

10 Appendix A – JSC Rendezvous Operations Procedures

Flight Rule C2-56:

SHUTTLE GO/NO GO FOR DOCKED OPERATIONS [RC]

A. IN ORDER TO BE GO TO CONTINUE DOCKED OPERATIONS, SHUTTLE PROPELLANT MUST BE AVAILABLE TO COVER THE FOLLOWING: ®[011801-7369]

1. SHUTTLE EMERGENCY UNDOCKING AND SEPARATION PER RULE {C4-152}, SHUTTLE/SOYUZ EMERGENCY UNDOCKING AND SEPARATION (TBV) [RC].

2. PROPELLANT REQUIRED FOR ORBITER MAINTENANCE (ATTITUDE CONTROL -ZLV -XVV OR THERMAL PROTECT ATTITUDE IF REQUIRED, 1 DEGREE VRCS, ONE IMU ALIGN/DAY) FOR 1 DAY.

3. DEORBIT REDLINES:

   a. OMS DEORBIT REDLINE (REF RULE {A6-303A}, OMS REDLINES [CIL])

   b. FRCS DEORBIT REDLINE (REF RULE {A6-304A}, FORWARD RCS REDLINES)

   c. ARCS ENTRY REDLINE (REF RULE {A6-305}, AFT RCS REDLINES)

B. IF SUFFICIENT PROPELLANT IS NOT AVAILABLE TO BE GO TO CONTINUE DOCKED OPERATIONS, UNDOCKING AT THE EARLIEST POSSIBLE OPPORTUNITY IS REQUIRED.

The ability to execute an immediate emergency undocking and separation, and subsequent deorbit to a Next Primary Landing Site (NPLS), is required in order to safely terminate the mission in the event of an emergency. This requires that sufficient propellant must be available post-undocking for attitude control until the next PLS deorbit opportunity (which could be up to 24 hours away). Note that if execution of the emergency undock and separation will increase the size of the deorbit burn, that increased delta V must be protected. ®[011801-7369]

FLIGHT/STAGE EFFECTIVITY: ALL FLIGHTS

Flight Rule C2-101:

ISS GO/NO-GO MATRIX FOR RENDEZVOUS [hc] [RC] ®[033105-6222D]

SYSTEM	FAILURE	NC FINAL	TI	PROX OPS	RPM [36]	R < 400 FT	R < 250 FT	R < 170 FT	DOCK
ISS	RS ARRAYS NOT IN REQUIRED POSITION FOR DOCKING	GO	GO	GO	GO	GO		DLY [2]	GO [2]
	USOS ARRAYS NOT IN REQUIRED POSITION FOR DOCKING	GO	GO	GO	GO	DLY [2]		GO [2]	GO [2]
	ISS IS NOT IN DOCKING ATTITUDE	GO	GO	GO [3]	NO-GO [26]	ABT [1]		ABT [1]	ABT [1]
	ISS TRACKING LIGHT	GO	GO [3]	GO	GO	GO		GO	GO
	ISS COMMUNICATION WITH GROUND	GO	TI DLY	ABT [18]	GO	ABT [18]		ABT [18]	ABT [18]
	ISS COMMUNICATION WITH ORBITER	GO	GO	GO	GO	GO		GO	GO
	ISS TRANSLATIONAL JETS NOT INHIBITED	GO	TI DLY	ABT [19]	NO-GO [19]	ABT [19]		ABT [19]	ABT [19]
	ISS SYSTEM FAILURE [7]		TI DLY	ABT	NO-GO	ABT		ABT	ABT
	PRIMARY C&C MDM		TI DLY [23]	GO	GO	DLY [23]		DLY [23]	DLY [23]
	PRIMARY GNC MDM (WHILE UNDER RS THRUSTER CONTROL)		GO	GO	GO	GO		GO	GO
	PRIMARY INT MDM		GO	GO	GO	GO [21]		GO [21]	GO [21]
	LA1 AND LA2 MDM'S		GO	GO	GO	GO [21]		GO [21]	GO [21]
	LOSS OF ATTITUDE CONTROL	GO	TI DLY (22)	GO	NO-GO [27]	ABT [24]		ABT [24]	ABT [24]
	DIGITAL STILL CAMERA (ALL ISS 400/800 MM↓)		GO	GO	NO-GO	GO		GO	GO
PROP/RCS	VRCS	GO	GO	GO	GO	GO	GO	GO	GO
	LAST AFT FIRING JET (+X)	GO	TI DLY [8]	ABT [32]	NO-GO [28]	ABT [32]	ABT [4]	ABT [4]	ABT [4]
	LAST FORWARD FIRING JET (-X)	GO	TI DLY [8]	ABT [32]	NO-GO [28]	ABT [32]	ABT [4]	ABT [4]	ABT [4]
	LAST FORWARD OR AFT LEFT FIRING JET (+Y)	GO	TI DLY [8]	GO [37]	NO-GO [28]	GO [37]	ABT [4]	ABT [4]	ABT [4]
	LAST FORWARD OR AFT RIGHT FIRING JET (-Y)	GO	TI DLY [8]	GO [37]	NO-GO [28]	GO [37]	ABT [4]	ABT [4]	ABT [4]
	LAST UP FIRING JET IN FORWARD OR EITHER AFT (+NZ)	GO	TI DLY [8]	GO	GO	GO	ABT [4]	ABT [4]	ABT [4]
	2 FORWARD FIRING JETS (DEGRADED -X, +LZ)	GO	GO [5]	GO [5]	GO [5]	GO [5]	GO [5]	GO [5]	GO [5]
	LAST AFT-FIRING JET IN EITHER POD (DEGRADED +X, +LZ)	GO	GO [5]	GO [5]	NO-GO [39]	GO [5]	GO [5]	GO [5]	GO [5]
	LAST DOWN FIRING JET ON EITHER SIDE OF FORWARD (+LZ PITCH AND PCT)	GO	TI DLY [8]	ABT [38]	[33]	ABT [38]	ABT [4, 6]	ABT [4, 6]	ABT [4, 6]
	LAST DOWN FIRING JET IN EITHER AFT POD (+LZ ROLL AND PCT)	GO	TI DLY [8]	GO [29]	NO-GO[34]	GO [29]	ABT [6]	ABT [6]	ABT [6]
	ANY SINGLE FWD DOWN FIRING JET OR ANY 2 DOWN FIRING JETS IN EITHER AFT POD	GO	GO	GO	NO-GO [38]	GO	GO	GO	GO
GNC									
IMU'S	2 ↓	GO	TI-DLY [8]	GO [35]	NO-GO [30]	GO [35]	ABT	ABT	ABT
CAMERAS	BOTH CENTERLINE/KEEL CAMERAS FAIL	GO	GO	GO	GO [40]	GO	ABT	ABT	ABT
TCS/HHL	ALL UNITS FAILED	GO	GO	GO	NO-GO [31]	GO	GO	ABT [20]	ABT [20]
CAMERA A & D	BOTH UNITS FAILED	GO	GO	GO	GO	GO	GO	GO	ABT [20]
STAR TRACKER	2 ↓	GO	GO	GO	GO	GO	GO	GO	GO
RNDZ RADAR	1 ↓	GO	GO	GO (IF VIS)	GO	GO	GO	GO	GO
COAS	1 ↓	GO	GO	GO	GO	GO	GO	GO	GO
ANGULAR ALIGN	ANGULAR ALIGNMENT CANNOT BE VERIFIED	GO	GO	GO	GO	GO	GO	GO	ABT
AFT THC CONTACTS	3 ± X ↓ OR 3 ± Y ↓ OR 2 -Z ↓	GO	TI-DLY [8]	ABT	NO-GO	ABT	ABT	ABT	ABT
FWD AND AFT	2 -Z FWD AND 2 -Z AFT ↓	GO [11]	GO [11]	GO	GO	GO	ABT	ABT	ABT
THC CONTACTS	4 +Z ↓	GO	TI-DLY [8]	GO	GO	GO	ABT [12]	ABT [12]	ABT [12]
DPS									
1 OF 3 GNC GPC'S	1 ↓	GO [9]	GO [9]	GO [9]	GO [9]	GO [9]	GO [9]	GO [9]	GO [9]
1 OF 2 GNC GPC'S	1 ↓	GO	TI-DLY	GO	NO-GO [30]	GO	ABT [10]	ABT [10]	ABT [10]
ANY GPC'S	2 ↓	GO [15]	ABT [14]	ABT [14]	NO-GO [14]	ABT [14]	ABT [14]	ABT [14]	ABT [14]
MDM (FF, FA, PL)	1 ↓	GO	GO	GO	GO [41]	GO	GO	GO	GO
SM GPC	1 ↓	GO [16]	GO [16]	GO [16]	GO [16]	GO [16]	GO [16]	GO [16]	GO [16]

®[062497-6019A] ®[040998-6450] ®[ED] ®[102398-6718C] ®[092800-7237] ®[110900-7370] ®[082301-4790B]
®[121902-5854] ®[042403-5929] ®[033105-6222D]

THIS RULE CONTINUED ON NEXT PAGE

C2-101 ISS GO/NO-GO MATRIX FOR RENDEZVOUS [HC] [RC] (CONTINUED)

NOTES:

[1] THE CORRIDOR APPROACH IS DESIGNED TO ENSURE PROXIMITY OPERATIONS ARE WITHIN THE LOADS DATABASE AND THAT TCS TARGETS ARE AVAILABLE. TO PROTECT THE RUSSIAN SOLAR ARRAYS, THE ORBITER CANNOT PROCEED CLOSER THAN 170 FT WITHOUT THE ISS BEING IN DOCKING ATTITUDE. STATIONKEEP AT OR BACKOUT TO 170 FT AND AWAIT THE ATTITUDE MANEUVER. TO PROTECT DEPLOYED U.S. SOLAR ARRAYS, THE ORBITER CANNOT PROCEED CLOSER THAN 400 FT. STATIONKEEP AT OR BACKOUT TO 400 FT AND AWAIT THE ATTITUDE MANEUVER IF U.S. SOLAR ARRAYS ARE DEPLOYED. WHEN U.S. SOLAR ARRAYS ARE DEPLOYED OUTBOARD OF S3 OR P3, THE U.S. CONSTRAINT IS EXPECTED TO INCREASE TO 600 FT. THIS WILL BE ASSESSED BEFORE 12A.1. ®[062497-6019A] ®[102398-6718C] ®[110900-7370] ®[121902-5854]

[2] GO IF SHUTTLE LOW Z IS AVAILABLE. ®[082301-4790B]

WITHOUT LOW Z:

DELAY APPROACH WITHIN 170 FT UP TO AN ORBIT IF POSSIBLE TO POSITION RUSSIAN SOLAR ARRAYS.

DELAY APPROACH WITHIN 400 FT UP TO AN ORBIT IF POSSIBLE TO POSITION U.S. SOLAR ARRAYS. OTHERWISE, PROCEED CLOSER WITHOUT ARRAYS BEING FEATHERED OR CONFIRMED NOT TO BE IN A KEEP-OUT ZONE.

REF RULES {C2-104}, ISS SYSTEM MANAGEMENT FOR APPROACH AND DOCKING [HC] [RC], AND {C2-109}, RNDZ/PROX OPS LOW Z/NORM Z MANAGEMENT [RC]. ®[082301-4790B]

[3] FOR FLIGHTS STARTING WITH 4A, IF THE TRACKING LIGHT FAILS, THEN THE ORBITER STAR TRACKERS WILL NOT BE AVAILABLE AS AN OPTIONAL SENSOR DURING THE RENDEZVOUS. THE USE OF THE STAR TRACKERS WITH THE TRACKING LIGHT ALSO REQUIRES THAT THE ISS IS IN AN ATTITUDE THAT ALLOWS USE OF THE TRACKING LIGHT BY TI + 28 MINUTES.

[4] ORBITER WILL NOT PROCEED INSIDE OR CONTINUE INSIDE 250 FT IF CONTROL IS COMPLETELY LOST IN ONE AXIS.

[5] SPECIAL CONDITIONS MUST BE MET TO CONTINUE INSIDE OF 1000 FT WITHOUT LOW Z BRAKING ABILITY. NO NORM Z BRAKING IS ALLOWED BETWEEN 1000 FT AND 75 FT. REF RULE {C2-109}, RNDZ/PROX OPS LOW Z/NORM Z MANAGEMENT [HC] [RC]. ®[ED]

[6] THE ORBITER CAN PROCEED WITH LOSS OF LOW Z ATTITUDE CONTROL. THE ORBITER SHOULD STAY VRCS IF AVAILABLE AND MODE TO NORM Z TAIL ONLY (IF AVAILABLE) AND NORM Z NOSE/TAIL OTHERWISE. HOWEVER, THE ORBITER CANNOT ATTEMPT A DOCKING IF PCT IS LOST. A GMEM OVERWRITE MUST BE IMPLEMENTED BEFORE THE ORBITER IS GO TO ATTEMPT A DOCKING. IF IN A "LOSS OF LOW Z ATTITUDE" OR "LOSS OF PCT" CASE, THE CONTROL IN THE -Z AND/OR ±Y AXES WILL ALREADY BE LOST, SO THE ORBITER WILL BE NO-GO INSIDE OF 250 FT. REF RULE {C2-109}, RNDZ/PROX OPS LOW Z/NORM Z MANAGEMENT [HC] [RC]. ®[ED]

[7] IF ANY ISS SYSTEMS FAIL (SUCH AS MCS, COMM, THERMAL, CDH, ETC.), WHICH WOULD PREVENT A SUCCESSFUL DOCKING OR VIOLATE DOCKING CONSTRAINTS, THE RENDEZVOUS WILL BE ABORTED. PRIOR TO TI, A TI DELAY MAY BE PERFORMED TO ALLOW TIME TO RECOVER THE FAILED SYSTEM. POST-TI, THE RENDEZVOUS WILL BE HALTED AT THE NEXT MOST CONVENIENT POINT. REFERENCE: HAZARD REPORT ISS-GNC-701-9A. ®[121902-5854] ®[033105-6222D]

[8] GO FOR TI IF CAPABILITY CAN BE RECOVERED PRIOR TO 250 FT WITHOUT IMPACTING RENDEZVOUS OPERATIONS. TI DELAY MAY BE PERFORMED TO PROVIDE MORE TIME TO EVALUATE THE SYSTEM FAILURE AND RECOVERY EFFORTS. ®[110900-7370]

[9] WHEN POSSIBLE, RESTRING TO REMAINING TWO GNC GPC'S. A RESTRING IS REQUIRED PRIOR TO THE RPM IN ORDER TO REGAIN REQUIRED JET REDUNDANCY. ®[033105-6222D]

[10] IF RANGE IS LESS THAN 250 FT, BACK OUT TO 250 FT AND RESUME APPROACH WHEN RECONFIGURED TO TWO GNC GPC'S.

[11] INCLUDES STRINGING. IF REDUNDANCY RECOVERABLE PRIOR TO 250 FT.

[12] GO IF EACH THC HAS ONE CONTACT REMAINING. ®[062497-6019A]

[13] RESERVED ®[110900-7370]

THIS RULE CONTINUED ON NEXT PAGE

C2-101 ISS GO/NO-GO MATRIX FOR RENDEZVOUS [HC] [RC] (CONTINUED)

[14] THIS ABORT CRITERIA IS BASED ON THE ASSUMPTION THAT AN SM AND A BFS MACHINE ARE REQUIRED AND THEREFORE NOT ENOUGH GPC'S ARE LEFT TO GET REDUNDANT GNC GPC'S. WITHOUT REDUNDANT GNC GPC'S, THE ORBITER IS NO-GO TO BURN TI OR TO PROCEED INSIDE OF 250 FT SO THERE IS NO REASON TO CONTINUE WITH THE RENDEZVOUS. IF THE SM OR BFS MACHINE COULD BE CONVERTED TO A GNC MACHINE, THEN THERE WOULD NOT BE ANY ABORT CRITERIA. (ADDITIONALLY, THIS FAILURE INVOKES AN MDF CONDITION ACCORDING TO THE FLIGHT RULES.)

[15] THIS FAILURE INVOKES AN MDF CONDITION ACCORDING TO THE FLIGHT RULES. ®[102398-6718C]

[16] WHEN POSSIBLE, GIVE UP 1 OF THE 3 GNC GPC'S AND FORM A NEW SM GPC. ®[102398-6718C]

[17] RESERVED

[18] WHILE AN ISS CREW IS ON-BOARD, RENDEZVOUS MAY PROCEED IF THE SHUTTLE AND ISS CREW HAVE VOICE COMMUNICATION AND CAN CONFIRM ISS SYSTEMS IN THE DOCK-READY CONFIGURATION. REF RULE {C2-106}, COMMUNICATIONS COVERAGE REQUIREMENTS DURING DOCKING OF SHUTTLE [HC] [RC]. IF THERE IS NO CREW ON-BOARD AND THE ABILITY FOR THE GROUND TO COMMUNICATE IS LOST, THE RENDEZVOUS WILL BE ABORTED. PRIOR TO TI, A TI DELAY COULD BE PERFORMED TO ALLOW TIME TO TRY TO RECOVER GROUND COMMUNICATION. POST-TI, THE RENDEZVOUS WILL BE HALTED AT THE NEXT MOST CONVENIENT POINT. ®[121902-5854]

[19] THE TRANSLATIONAL JETS ON THE ISS MUST BE INHIBITED TO PREVENT OVERPRESSURE OR THERMAL DAMAGE TO THE SHUTTLE DUE TO POTENTIAL ISS JET EXHAUST PLUME. IF THE TRANSLATIONAL JETS ON THE ISS CANNOT BE INHIBITED, THEN THE RENDEZVOUS WILL BE ABORTED. PRIOR TO TI, A TI DELAY COULD BE PERFORMED TO ALLOW TIME TO TRY TO INHIBIT THE JETS. POST-TI, THE RENDEZVOUS WILL BE HALTED PRIOR TO ENTERING PROXIMITY OPERATIONS.

[20] TO CONTINUE THE APPROACH (BETWEEN 170 FT AND 10 FT) WITH NO TCS/HHL UNITS OR TO PROCEED INSIDE 10 FT WITHOUT CAMERA A OR D WILL MEAN APPROACHING OUTSIDE THE BOUNDS OF PLUME, PROP AND CONTACT CONDITIONS ANALYSIS. CONSIDERATION CAN BE GIVEN TO CONTINUING THE APPROACH WITH THE ACCEPTANCE OF POTENTIALLY SEVERE IMPACTS TO PLUME LOADING ON THE STATION APPENDAGES, SHUTTLE PROPELLANT MARGINS, AND CONTACT CONDITIONS. ®[102398-6718C] ®[110900-7370]

[21] IF ACS AUTO-MODING SOFTWARE/LIGHTS CANNOT BE CONFIGURED TO SUPPORT AUTOMATIC MODING AT CONTACT, OR IF PRIMARY INT MDM FAILS, OR IF BOTH LA1 AND LA2 MDM'S FAIL, CONTINUE APPROACH WITH ISS CREW DESIGNATED PRIME AND MCC-H/M DESIGNATED BACKUP FOR COMMANDING ISS TO FREE DRIFT UPON "CAPTURE CONFIRMED." ®[082301-4790B]

[22] "GO FOR TI" REQUIREMENTS DICTATE ISS MUST BE IN A KNOWN CONFIGURATION CAPABLE OF ACHIEVING THE DOCKING ATTITUDE WITH LVLH RATES OF 0.04 DEG/SEC PER AXIS OR LESS.

[23] C&C MDM FAILURE TAKES DOWN ALL AUTOMATIC MODING (OF BOTH USOS AND RS) AND MANUAL USOS COMMANDING TO FREE DRIFT, AS WELL AS ALL USOS COMMAND AND TELEMETRY. IN THE CASE WHERE RUSSIAN MANUAL MODING IS REQUIRED, THE CREW SHALL HAVE ACCESS TO A RUSSIAN LAPTOP OR ISS MAY BE OVER A RUSSIAN GROUND SITE. REFER TO RULE {C2-104}, ISS SYSTEM MANAGEMENT FOR APPROACH AND DOCKING [HC] [RC], AND RULE {C2-106}, COMMUNICATIONS COVERAGE REQUIREMENTS DURING DOCKING OF SHUTTLE [HC] [RC]. A C&C MDM SHOULD AUTOMATICALLY BE RECOVERED WITHIN 5 SECONDS, WHICH WILL PROVIDE TELEMETRY AND GROUND COMMANDING. THE ISS CREW WOULD HAVE TO RECONNECT THE PCS FOR COMMAND AND TELEMETRY CAPABILITY.

[24] THE ORBITER WILL PERFORM A CORRIDOR BACKOUT TO 400 FT ON +VBAR TO MITIGATE SHUTTLE PLUME AND COLLISION CONCERNS IF ISS DRIFTS OUT OF ATTITUDE. THE ORBITER MAY CONTINUE IN FROM 400 FT ONCE ISS HAS ASSUMED ATTITUDE CONTROL AND IS BACK IN THE DOCKING ATTITUDE. REFERENCE: HAZARD REPORT ISS-GNC-701-9A. ®[121902-5854] ®[033105-6222D]

[25] GO IF ATTITUDE CONTROL IS HANDED OVER TO THE SM. ACS MODING WILL STILL FUNCTION. IF TIME ALLOWS, PREPARE FOR MCC-M BACKUP COMMAND. ®[082301-4790B]

[26] RELATIVELY SMALL EXCURSIONS FROM THE DOCKING ATTITUDE COULD OBSCURE THE VIEW FROM THE ISS WINDOW. IN ADDITION, PLUME LOADS ON ISS HAVE ONLY BEEN ANALYZED FOR THE DOCKING ATTITUDE.

[27] CONTINUE TO 400 FT ON VBAR TO AWAIT TROUBLESHOOTING. ®[033105-6222D]

THIS RULE CONTINUED ON NEXT PAGE

C2-101 ISS GO/NO-GO MATRIX FOR RENDEZVOUS [HC] [RC] (CONTINUED)

[28] POSITIVE CONTROL IS REQUIRED IN EACH AXIS IN ORDER TO SET UP THE INITIAL CONDITIONS FOR THE RPM. ®[033105-6222D]

[29] LOSS OF PRCS LOW Z ROLL CONTROL. GO AS LONG AS VERNS ARE AVAILABLE.

[30] CRITICAL VEHICLE CONTROL SYSTEMS MUST BE REDUNDANT TO SAFELY PERFORM THE RPM.

[31] USE OF TCS OR HHL IS REQUIRED TO MEET THE RANGE AND RANGE RATE CONDITIONS SPECIFIED FOR STARTING THE PITCH MANEUVER. ATTEMPTING THE MANEUVER WITHOUT MEETING THESE CONDITIONS COULD ALLOW LARGE TRAJECTORY DISPERSIONS TO BUILD DURING THE MANEUVER. RECOVERY FROM THESE DISPERSIONS COULD BE PROPELLANT-EXPENSIVE, AND WOULD BE FURTHER COMPLICATED BY THE UNAVAILABILITY OF THE TCS AND HHL SENSORS. SINCE HHL RAW RANGE RATE AT THE RPM RANGE HAS BEEN SHOWN TO BE HIGHLY DEPENDENT ON OPERATOR TECHNIQUES, CONSECUTIVE RANGE MARKS SHOULD BE USED TO ESTIMATE RANGE RATE. THE RPOP HHL/DT FUNCTION IS PREFERRED FOR THIS METHOD. (REFERENCE ORBIT FLIGHT TECHNIQUES PANEL #217, JANUARY 28, 2005.)

[32] BOTH ±X TRANSLATIONS ARE REQUIRED TO STABILIZE ON THE +RBAR, TO START AND STOP THE TWICE ORBITAL RATE VBAR APPROACH (TORVA), AND TO MAINTAIN THE VBAR.

[33] THE RPM IS ALREADY NO-GO FOR LOSS OF THE FIRST FORWARD DOWN-FIRING JET (SEE NOTE [38]).

[34] IF ALL DOWN-FIRING JETS IN THE SAME AFT POD ARE FAILED, THERE IS NOT ADEQUATE PRCS CONTROL AUTHORITY TO NULL THE PITCH RATE. THE TORVA IS FLYABLE IN LOW Z IN THIS CASE ONLY IF VERN JETS ARE AVAILABLE. OTHERWISE, ROLL CONTROL IS COMPLETELY LOST.

[35] ONCE TI IS EXECUTED, A LOSS OF SYSTEMS REDUNDANCY IS NOT CAUSE TO ABORT/BREAKOUT IF THE SYSTEM CAN BE RECOVERED AT THE NEXT CONVENIENT HOLDING POINT (ALTHOUGH CERTAIN REDUNDANCY REQUIREMENTS EXIST FOR THE RPM).

[36] THIS COLUMN DEFINES THE GO/NO-GO CRITERIA FOR STARTING THE RPM.

[37] ALTHOUGH ±Y CAPABILITY IS LOST, LARGE Y EXCURSIONS ARE NOT EXPECTED DURING THIS TIMEFRAME. ALSO, INCREASED CLOSURE FROM CROSS-COUPLING WOULD NOT BE SIGNIFICANT IN THIS JET CONFIGURATION.

[38] WITH TWO FORWARD DOWN-FIRING JETS LOST ON ONE SIDE, ±Y AND LOW Z BRAKING CAPABILITY IS LOST. LARGE CLOSURE MAY DEVELOP DUE TO DEGRADED PRCS LOW Z ATTITUDE CONTROL. STARTING THE RPM WILL CAUSE A LARGE CLOSING RATE TOWARD ISS THAT WILL FORCE A BREAKOUT FROM THE RENDEZVOUS. WHILE THIS BREAKOUT TRAJECTORY PROVIDES ADEQUATE CLEARANCE BETWEEN THE ORBITER AND THE ISS (> 170 FT), THERE MAY NOT BE ENOUGH PROPELLANT TO PERFORM A RE-RENDEZVOUS. TO PRECLUDE THE POSSIBILITY OF A BREAKOUT, REDUNDANT FORWARD DOWN-FIRING JETS ARE REQUIRED FOR THE RPM. (REFERENCE ORBIT FLIGHT TECHNIQUES PANEL #216, NOVEMBER 19, 2004.) ®[ED]

FAILURE OF THE REMAINING DOWN-FIRING AFT JET DURING THE RPM WOULD RESULT IN A LOSS OF LOW Z PRCS PITCH CONTROL (SEE NOTE [34]).

[39] PERFORMING THE RPM WITH ONLY ONE +X JET COULD COMPLICATE THE TRANSITION FROM THE RPM INTO THE TORVA.

[40] CAMERA A OR D CAN BE ALIGNED ALONG THE -Z AXIS TO BE USED AS A CENTERLINE CAMERA SUBSTITUTE FOR SETTING UP THE RPM INITIAL CONDITIONS.

[41] THE OTHER SYSTEMS PORTIONS OF THE TABLE SHOULD BE CONSULTED TO DETERMINE RENDEZVOUS IMPACTS FROM LOSS OF SYSTEMS ASSOCIATED WITH THE AFFECTED MDM.

Reference: Hazard Report ISS-COLL-1003-11A, Hazards during Proximity Operations.
®[033105-6222D]

FLIGHT/STAGE EFFECTIVITY: 11A AND SUBS ®[ED]

Flight Rule C2-104:

ISS system management for approach and docking [HC] [RC] ®[052401-7518]

A. ISS APPENDAGE CONFIGURATION: ®[110900-7370]

1. NOMINALLY, THE P6 4B SOLAR ARRAY WILL BE FIXED AT 210 DEGREES AND THE P6 2B SOLAR ARRAY WILL BE FIXED AT 150 DEGREES FOR ORBITER APPROACH WITHIN 400 FEET. THE BGA'S WILL NOT BE LATCHED AND THE DRIVE MOTORS WILL REMAIN POWERED WITH THE BGA MODE SET TO DIRECTED POSITION. ®[092701-4792D]

This Rule defines the P6 array positions for approach and docking. Boeing-ISS loads, and thermal and control analyses have shown there are no requirements to lock the BGA's for dockings to the PMA2 on the Lab Forward CBM.

2. NOMINALLY, THE FGB AND SM SOLAR ARRAYS WILL BE FIXED IN SUN ZONE 1 OR 9 FOR ORBITER APPROACH WITHIN 170 FEET.

This Rule defines the SM and FGB array positions for approach and docking.

3. THE SHUTTLE WILL DELAY APPROACH UP TO ONE ORBIT, PROPELLANT ALLOWING, STATIONKEEPING TO ALLOW ISS SOLAR ARRAYS TO BE ORIENTED TO THE POSITIONS DEFINED ABOVE. IF THE 2B OR 4B ARRAY IS WITHIN A RANGE OF ±5 DEG FROM WHAT IS DEFINED IN PARAGRAPH 1 ABOVE, DOCKING MAY CONTINUE WITHOUT DELAY.

The ±5 deg angle range will only be used if the array cannot be positioned nominally as a result of a BGA positioning problem. Any position between the ±5 deg range is sufficient to protect the array against departure loads.

4. IF THE USOS OR RS ARRAYS CANNOT BE ORIENTED IN THE POSITIONS DEFINED ABOVE, APPROACH AND DOCKING MAY PROCEED WITH OR WITHOUT LOW Z BRAKING. NO NORM Z BRAKING IS ALLOWED BETWEEN 1000 FT AND 75 FT.

There are no loads or thermal keepout zones for dockings to the PMA2 on the Lab Forward CBM. Special conditions must be met to continue inside of 1000 ft without Low Z braking ability. Reference Rule {C2-109}, RNDZ/PROX OPS LOW Z/NORM Z MANAGEMENT [HC] [RC].
®[092701-4792D] ®[ED]

THIS RULE CONTINUED ON NEXT PAGE

C2-104 ISS SYSTEM MANAGEMENT FOR APPROACH AND DOCKING [HC] [RC] (CONTINUED)

Loads analyses indicate shuttle plume loads within 170 feet could exceed Russian solar array load limits and, within 400 feet, could exceed U.S. solar array load limits if the arrays are not locked. It should be noted that if the U.S. solar arrays are not feathered, a TORVA from the +Rbar during approach should be initiated by 600 feet to ensure the orbiter is no closer than 400 feet at Vbar arrival. ®[032901-7485]

Reference: Hazard Report ISS-MCH-109. ®[092701-4792D]

FLIGHT/STAGE EFFECTIVITY: 2A THROUGH 12A

B. STATION-ORBITER ATTITUDE CONTROL SYSTEM MODING AT DOCKING

1. AT LEAST ONE COMMAND SOURCE SHALL BE AVAILABLE TO MODE THE STATION INTO FREE DRIFT. ®[032901-7485]

2. THE LIST OF COMMAND SOURCES INCLUDES THE FOLLOWING IN ORDER OF PRIORITY:

PRIORITY	COMMAND SOURCE
1.	AUTOMATIC ACS MODING IN THE CCS
2.	ISS CREW
3.	GROUND (MCC-H OR MCC-M)

®[032901-7485] ®[092701-4792D]

3. IF THE ISS IS NOT IN FREE DRIFT 20 SECONDS AFTER THE ORBITER CREW CALL OF CAPTURE CONFIRMED, ANY BACKUP COMMAND SOURCE SHALL COMMAND THE ISS TO FREE DRIFT. ®[302901-7485] ®[121902-5855]

The automatic ACS moding is the first priority command source. The automatic ACS moding shall be considered a single, redundant command source, since the ACS moding status is not checkpointed to the backup C&C MDM. The highest priority available command source is considered the primary command source. The ISS crew is higher priority than the ground to protect for a loss of communication.

For the case of the Service Module in attitude control and MCC-M or ISS crew needing to command the ISS to free drift, the ISS crew shall send the Russian command that is an imitation of the arrival event and completes the docking cyclogram. MCC-M commanding may go through U.S. assets, otherwise docking over a Russian Ground Site may be considered. Reference Rule {C2-106}, COMMUNICATIONS COVERAGE REQUIREMENTS DURING DOCKING OF SHUTTLE [HC] [RC]. ®[092701-4792D] ®[302901-7485] ®[121902-5855]

THIS RULE CONTINUED ON NEXT PAGE

C2-104 ISS SYSTEM MANAGEMENT FOR APPROACH AND DOCKING [HC] [RC] (CONTINUED)

The 20-second delay will allow ample time to evaluate the success of the primary command source and will still provide time for the manual command to be executed. The 20 seconds provides sufficient time for the docking mechanism signals to reach the C&C MDM, internal processing and commanding to the U.S. GNC MDM and RS TC, and telemetry feedback to the operator. The 20-second delay is also due to MCC-M's concern that problems may occur if commands are received simultaneously from more than one of the several sources. If ACS Moding is not expected to operate due to failures such as an INT MDM at Dock minus 5 minutes, either LA MDM's, or Node MDM's out of sync, it is not necessary to wait 20 seconds. ®[302901-7485] ®[121902-5855]

4. IF THE ORBITER CREW HAS NOT RECEIVED POSITIVE CONFIRMATION OF ISS FREE DRIFT BEFORE CAPTURE +65 SECONDS, THEN THE ORBITER CREW WILL OPEN THE LATCHES AND PERFORM THE FAILED CAPTURE PROCEDURE. POSITIVE CONFIRMATION CAN COME FROM ANY OF THE FOLLOWING:

   a. ISS CREW

   b. ORBITER CREW, BASED ON THE FLASHING LED'S, OR FROM THE ARR/DPRTR MODING SPEC

   c. MCC-H ®[032901-7485]

   d. MCC-M, IF THE SERVICE MODULE WAS IN CONTROL (CALL RELAYED VIA MCC-H)

If the ISS has not moded to free drift within 65 seconds of capture, the docking mechanism load limits may be exceeded. Reference ES/J. Dagen, for 4A and subs.

If the LED is steady on, then the station is in attitude control. If the LED is flashing, then the station is in free drift. Failures exist that would prevent the LED from flashing. These failures would leave the LED's either in a powered-off state or in a steady-on state. There is no failure that could cause the LED's to falsely indicate free drift (per SPN 285). ®[032901-7485] ®[121902-5855]

Reference: Hazard Report ISS-MCH-109. ®[092701-4792D]

FLIGHT/STAGE EFFECTIVITY: 2A THROUGH 12A ®[ED]

THIS RULE CONTINUED ON NEXT PAGE

C2-104 ISS SYSTEM MANAGEMENT FOR APPROACH AND DOCKING [HC] [RC] (CONTINUED)

C. THE ISS KU-BAND SYSTEM SHALL BE OPERATED IN AUTOTRACK MODE WITH THE ANTENNA "SHUTTLE MASK" ENABLED BY RANGE = **TBD** METERS. ®[110900-7370]

Reference: Hazard Report ISS-MCH-109. ®[092701-4792D]

FLIGHT/STAGE EFFECTIVITY: ALL FLIGHTS

D. SOLAR ARRAY SUN TRACKING SHALL BE RESUMED WHEN CAPTURE IS CONFIRMED AND ISS IS IN FREE DRIFT.

After capture and ISS modes to free drift, the mated stack is in a safe configuration and a subsequent separation is unlikely. Therefore, sun tracking will be initiated as soon as possible to allow ISS to recover from the rendezvous power down. ®[110900-7370]

E. REFER TO RULE {B2-19}, U.S. LAB WINDOW OPERATIONAL CONSTRAINTS, FOR MANAGEMENT OF THE LAB SHUTTER DURING SHUTTLE DOCKING.

F. SSRMS SHALL BE IN A PRE-ANALYZED DOCKING CONFIGURATION. ®[092701-4792D]

FLIGHT/STAGE EFFECTIVITY: ALL FLIGHTS

Flight Rule C2-105:

Shuttle SENSOR REQUIREMENTS for ISS prox ops [RC] ®[CR 4885] ®[102398-6753A] ®[ED] ®[110900-7370]

A. FOR ISS FINAL APPROACH AND DOCKING OPERATIONS, THE FOLLOWING SENSORS ARE REQUIRED TO ENSURE THAT DOCKING CAN BE ACCOMPLISHED WITHIN THE BOUNDS OF ISS STRUCTURAL LOAD LIMITS, THE SHUTTLE APPROACH PROPELLANT BUDGET, AND THE DOCKING WINDOW:

A TRAJECTORY CONTROL SENSOR (TCS) OR HAND-HELD LIDAR (HHL), AND

A CENTERLINE CAMERA, AND

A PAYLOAD BAY CAMERA WITH AN ASSOCIATED MONITOR OVERLAY TO BE USED FOR RANGE/RANGE RATE DETERMINATION

Parametric database analysis has shown that successful docking can be consistently achieved with the use of TCS or HHL in combination with a centerline camera and payload bay bulkhead camera. Without a centerline camera, proper lateral and angular alignment to ensure a successful docking cannot be guaranteed. Without a TCS or HHL, the proper range/range rate profile and approach timing cannot be flown. Use of a payload bay camera with an unobstructed view of the docking interface (typically camera A or D) in conjunction with a monitor overlay is required in order to achieve the specified closing rate during the last few feet of approach given the data latency associated with using either TCS or HHL in conjunction with RPOP. Additionally, TCS reflector obscuration and HHL minimum range constraints may make these sensors unusable the last few feet of approach.

This rule documents the minimum sensor configuration used in docking database generation. A successful docking may be possible without one or more of these sensors given a wide margin for error in the propellant budget, plume loads, docking loads, capture probability, and docking time.

1. PRIOR TO DOCKING, THE APPROACH WILL BE ABORTED AND A CORRIDOR BACKOUT INITIATED IF REGAINING A REQUIRED DOCKING SENSOR IS POSSIBLE.

If regaining one or more of the required docking sensors is possible, then it is prudent to abort the approach in an effort to regain those sensors (via centerline camera replacement, TCS thermal conditioning, HHL IFM, etc.). Performing a corridor backout while sensor troubleshooting is underway will minimize plume loads on the ISS. ®[102398-6753A]

THIS RULE CONTINUED ON NEXT PAGE

C2-105 SHUTTLE SENSOR REQUIREMENTS FOR ISS PROX OPS [RC] (CONTINUED)

2. IF THE FULL COMPLEMENT OF REQUIRED SENSORS CANNOT BE REGAINED, CONSIDERATION WILL BE GIVEN TO CONTINUING THE APPROACH TO DOCK ON A BEST EFFORT BASIS WITH THE INCREASED POSSIBILITY OF EXCEEDING ISS STRUCTURAL LOAD LIMITS. ®[102398-6753A]

Continuing the approach to dock without the full complement of docking sensors significantly increases the risk of exceeding ISS structural load limits. Specifically, the degraded sensor complement can lead to approach trajectories and shuttle jet firings that are outside of analyzed performance envelopes, resulting in plume loads that exceed ISS solar array structural limits. Furthermore, contact conditions may be sufficiently off nominal that the ISS structural integrity is compromised or the docking mechanism is damaged to an extent that further dockings are not possible. These risks to ISS hardware must be weighed against mission objectives when deciding whether to continue the approach.

FLIGHT/STAGE EFFECTIVITY: 2A.1 AND SUBS

B. FOR ISS UNDOCKING OPERATIONS, A SENSOR CAPABLE OF MEASURING ISS LATERAL DISPLACEMENT FROM THE ORBITER DOCKING MECHANISM CENTERLINE IS REQUIRED.

When the orbiter undocks and departs from the ISS, the pilot must maintain the ISS within an 8 deg corridor relative to the orbiter docking mechanism centerline, necessitating the use of a centerline camera or equivalent sensor. This corridor separation ensures ISS structural load limits are not exceeded as a result of orbiter jet firings. For failure of the primary centerline camera, the backup centerline camera should be installed to support undocking operations. It is also possible, depending on the ISS configuration, to use other cameras (bulkhead camera or camcorder) or the COAS in conjunction with procedural updates to support orbiter undocking. For example, ISS structure that is centered in the COAS when the orbiter is positioned in the 8 deg corridor can be used as a corridor reference. TCS in conjunction with RPOP is also capable of providing corridor position but is subject to reflector visibility. ®[102398-6753A]

THIS RULE CONTINUED ON NEXT PAGE

C2-105 SHUTTLE SENSOR REQUIREMENTS FOR ISS PROX OPS [RC] (CONTINUED)

C. FOR ISS FLYAROUND OPERATIONS, A FUNCTIONAL HAND-HELD LIDAR (HHL) IS REQUIRED. ®[102398-6753A]

Flyarounds require the pilot to maintain a prescribed range from a specific target on the ISS. KU Radar is not considered a valid sensor to support flyaround operations because of the degraded measurements resulting from beam wandering over the length of the ISS. TCS is not considered a valid sensor to support flyaround operations because TCS reflectors are not visible at all times during a flyaround. The only sensor that provides precise ranging to specific targets on the ISS at all times is the HHL. Without an accurate ranging sensor, a flyaround at a specific range cannot be maintained. Plume loads analysis and propellant budgets assume range limits are maintained during flyaround operations.

A centerline camera, although desirable, is not required to support a flyaround. At flyaround range, use of the COAS or other payload bay cameras is adequate to support flyaround operations.

1. IF A FUNCTIONAL HHL IS NOT AVAILABLE PRIOR TO THE START OF A FLYAROUND, THEN THE FLYAROUND WILL NOT BE PERFORMED.

2. IF THE LAST FUNCTIONING HHL FAILS DURING A FLYAROUND, THE FLYAROUND WILL BE ABORTED AND A BREAKOUT MANEUVER PERFORMED.

If a functional HHL is not available during a flyaround, then a breakout must be initiated as agreed at Generic Joint Operations Panel #48 on March 10, 1998. ®[102398-6753A]

FLIGHT/STAGE EFFECTIVITY: ALL FLIGHTS

11 Appendix B – GSFC Automated Fault Protection

Missions run by Goddard typically use a combination of Telemetry Statistical Monitors (TSMs) and Fault Detection and Correction (FDC) for fault protection. These operate at the spacecraft or system level, and at the subsystem level respectively. The following discussion is in the context of the Power Subsystem Electronics (PSE) [10], a subsystem on EO-1.

11.1 Automated Spacecraft Response: Telemetry Statistical Monitors (TSMs)

The Telemetry Statistical Monitor (TSM) system is resident within the Mongoose V Command and Data Handling (C&DH) Processor. It provides fault protection across all subsystems, including PSE. The matrix of all TSMs flying on EO-1 is shown in the ASIST workstation display in **Figure 1**.

Two levels of automatic fault protection are handled by TSMs. If these do not prevent the progress of the fault, a third level of automatic protection is provided by the FDC actions at the PSE subsystem Remote Service Node (RSN). There are four TSMs and RTS responses in the automatic protection system for power. The TSM actions will take place when out-of-limit conditions are experienced for Battery Differential Voltage, Battery Low Voltage, Battery High Temperature, and Battery Low State of Charge. For example, TSM #050 checks for low Battery State of Charge (BSOC):

If BSOC < 85%, issue event message

If BSOC > 30% and BSOC < 70%,
call Safe Power (RTS #19)

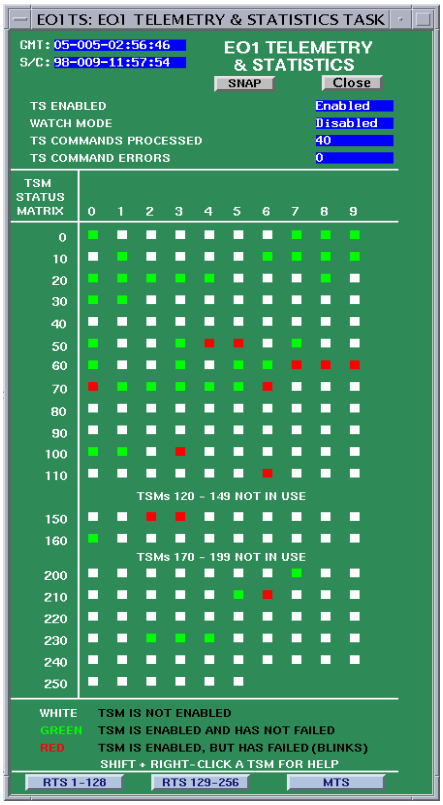


Figure 1: EO-1 TSM Matrix

When the parameter being monitored by the TSM exceeds the first (most sensitive) level of limit violation, the TSM will issue a limit violation event message after three consecutive violations. If the parameter telemetry value continues to degrade and the out-of-limit reading exceeds the second limit level (more severe violation), the TSM will issue a series of preprogrammed commands to attempt to protect the spacecraft and correct the limit violation. The commands initiated by the TSM are Relative Timed Sequence (RTS) commands, designated by individual sequence numbers. For TSM #050, RTS #19 initiates the loadshed and safehold sequence.

TSMs can be individually enabled and disabled. If a TSM often generates false positives, it can be disabled until a patch to the spacecraft software can be uploaded. This can also be used to allow the operators of the spacecraft to perform actions that were not

envisioned at design time, but are later determined to be necessary and safe. For example, one TSM is tripped when the spacecraft instrument covers are open and the spacecraft begins to point toward the sun, which will damage the instruments. However, this maneuver is allowable when the spacecraft is in the Earth's shadow. When the maneuver is necessary and safe, this TSM is disabled, then re-enabled after the maneuver is complete.

The TSM matrix is inherently a non-intuitive user interface – unless the operator knows the TSM matrix very well, it does not provide insight at a glance. The operator must examine each effected TSM to determine the problem. TSMs do not identify root cause. A common failure – e.g., power – would cause the display to light up like a Christmas tree, as in **Figure 1**.

The number of TSMs implemented for EO-1 was limited due to development effort and cost. Scalability is a challenge for rule-based systems, due to the lack of structure in the set of Fault Protection rules.

11.2 Automated Subsystem Response: Fault Detection and Correction (FDC)

FDCs provide health management local to each subsystem. The PSE RSN processor continuously monitors the power system spacecraft telemetry and automatically responds to certain telemetry limit violations in a similar but not identical fashion as the automated TSM response. The limits for the FDC are set to more extreme (forgiving) levels than the stricter TSM limits, the idea being that the FDC will kick in should the TSM fail to act. The logic flow chart for the 3 PSE FDCs is shown in **Figure 2** below.

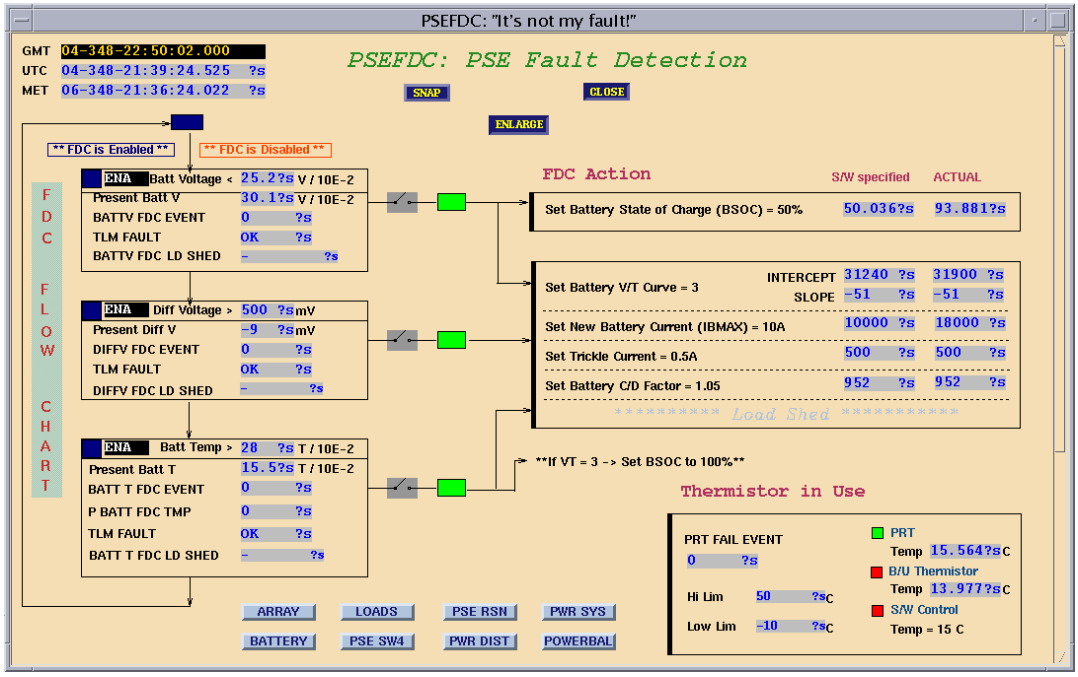


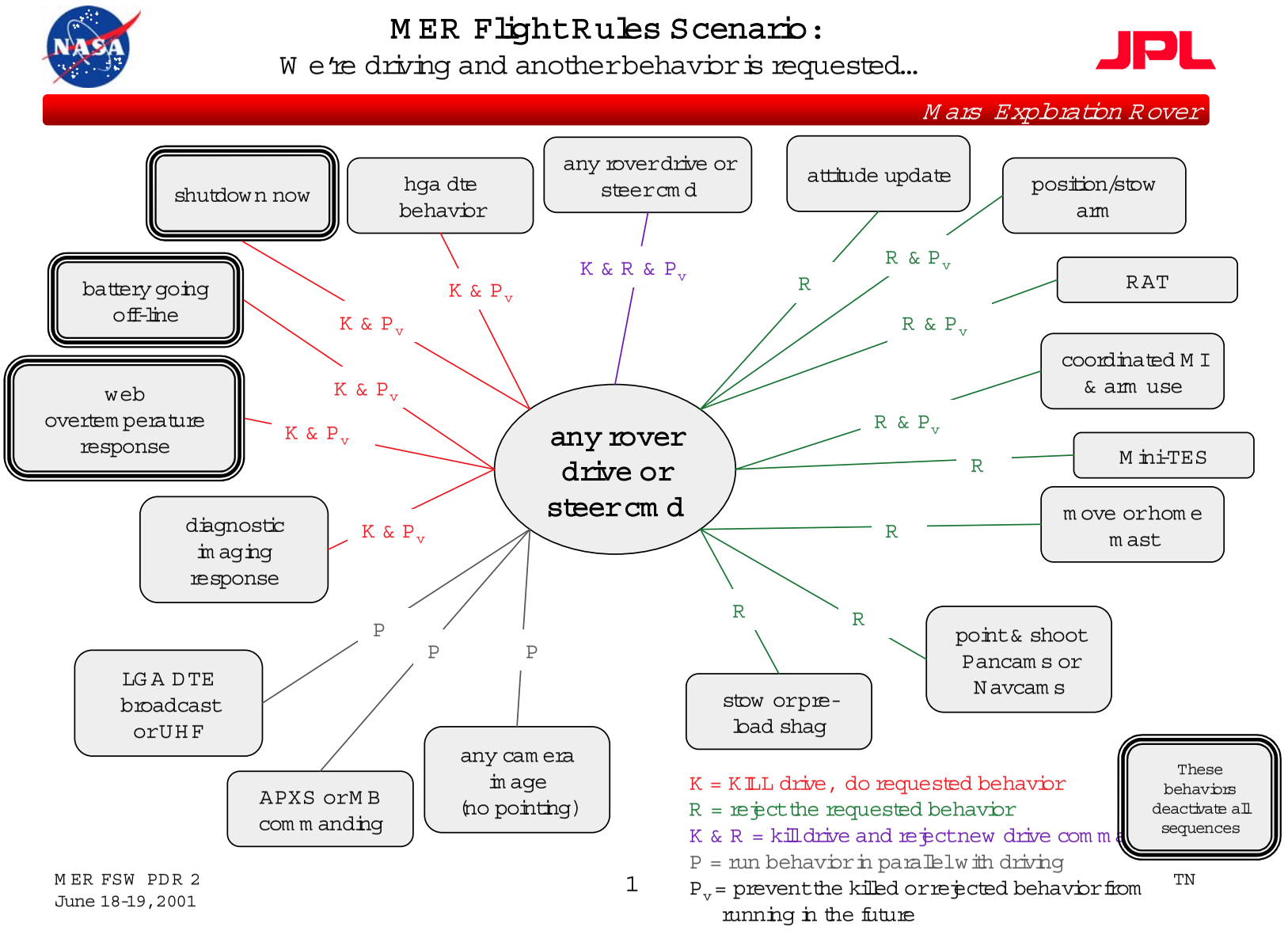
Figure 2: EO-1 FDCs for the Power Subsystem Electronics

TSMs, with their stricter redlines, normally perform all loadshedding and safehold, since the PSE FDCs cannot load shed other subsystems. The PSE FDCs serve as a backup should the TSMs fail to trip. Each trigger on the left is linked to the corrective action(s) on the right. The first FDC corresponds to the low BSOC TSM #050. This FDC will trigger two actions if battery voltage drops below 25.2V. First it sets BSOC to 50% to force triggering of TSM #050 if it did not already trip for some reason. Second, a series of steps lower the battery charge rate to implement loadshedding by setting the Voltage/Temperature curve to 3 (normally the charge rate is 4.5). In addition, several parameters are set to their normal values: battery maximum current is set to 10A to prevent overcharging; trickle current is set to nominal 0.5A; and the battery C/D (charge/discharge) factor is set to 1.05, reflecting the fact that the battery is not perfectly efficient.

The FDC automated response was designed for redundancy, so that spacecraft protection was still available from the subsystem RSN in the event the TSM protection at C&DH was malfunctioning. However, there is a potential for TSM/FDC conflict – it is quite possible that an FDC limit violation may occur after a valid TSM limit response was issued. In this case, TSM and FDC responses will be operating in parallel. The FDC and TSM responses had to be designed so that there are no conflicts between the two systems.

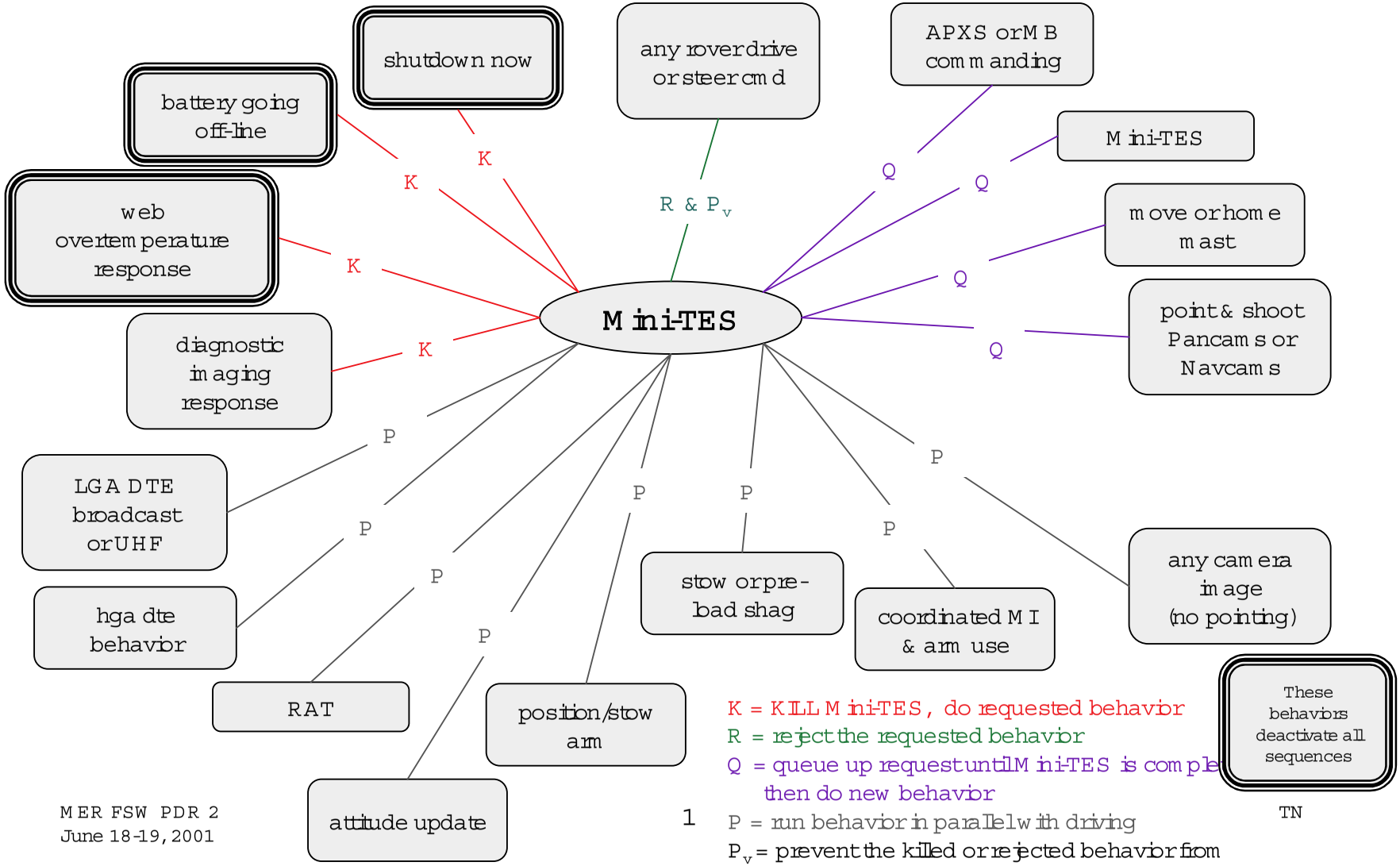
Another limitation is that FDC corrective actions are limited to the scope of the subsystem, and any impact on other subsystems must be handled by TSMs. If system-level response is required, a TSM must be tripped to initiate wider recovery of the spacecraft. In this way the FDC which sets BSOC = 50% will trip TSM #50 to do load shedding and safehold. This relationship is implicit, and if improperly managed could result in unexpected behavior with potentially severe consequences.

12 Appendix C – JPL Mars Exploration Rover Flight Rules



MER Flight Rules Scenario:

We're Mini-TESing and another behavior is requested...



Surface Ops Behavior Relationships Matrix

Mars Exploration Rover

"A" is active and "B" is requested			camera		x				x	x			x	x	
			payload interface												
				2	4	5	6	7	8	10	11	12	14	16
			"B" Behaviors / behavior category / "A" Behaviors	LGA DTE communication	attitude acquisition/update for HGA communications	HGA DTE communication	UHF communications	stow SHAG/ pre-load for drive	attitude acquisition/update for mobility and science	any rover drive or steer cmd	position/stow arm	any Mössbauer Spectrometer commanding & data transfer	any APXS commanding & data transfer	RAT (expose surface)
		2	LGA DTE communication	WTS conflict - kill & service new	no conflict	WTS conflict - kill & service new	telecom board conflict - kill & service new	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict
x		4	attitude acquisition/update for HGA communications	no conflict	shag conflict - reject new	shag conflict, kill & service new	no conflict	shag conflict - kill current & service new	shag conflict - kill current & service new	motor conflict - kill current & prevent future, service new	no conflict	no conflict	no conflict	no conflict
		5	HGA DTE communication	WTS conflict - kil & service new	shag conflict, kill & service new	shag conflict, kill & service new	telecom board conflict - kill & service new	shag conflict - kill current & service new	shag conflict - kill current & service new	motor conflict - kill current & prevent future, service new	no conflict	no conflict	no conflict	no conflict
		6	UHF communications	telecom board conflict - kill & service new	no conflict	telecom board conflict - kill & service new	intent conflict - kill & service new	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict
		7	stow SHAG/ pre-load for drive	no conflict	shag conflict - reject new	shag conflict - reject new	no conflict	shag conflict - reject new	shag conflict - reject new	motor conflict - reject new	no conflict	no conflict	no conflict	no conflict
x		8	attitude acquisition/update for mobility and science	no conflict	shag conflict - reject new	shag conflict - reject new	no conflict	shag conflict - reject new	shag conflict - reject new	motor conflict - reject new	no conflict	no conflict	no conflict	no conflict
x		10	any rover drive or steer cmd	no conflict	motor conflict - reject new & prevent	motor conflict - reject new & prevent	no conflict	motor conflict - reject new & prevent	motor conflict - reject new & prevent	danger - kill current, reject new & prevent	motor conflict - reject new & prevent	no conflict	no conflict	motor conflict - reject new & prevent
		11	position/stow arm	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	motor conflict - reject new & prevent	danger - kill current, reject new & prevent	no conflict	no conflict	danger - kill current, reject new & prevent
	x	12	any Mössbauer Spectrometer commanding & data transfer	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	payload conflict - queue	payload conflict - queue	no conflict
	x	14	any APXS commanding & data transfer	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	payload conflict - queue	payload conflict - queue	no conflict
		16	RAT (expose surface)	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	motor conflict - reject new & prevent	danger - kill current, reject new & prevent	no conflict	no conflict	RAT conflict - queue
x		17	coordinated Microscopic Imager & arm use	no conflict	camera conflict - queue	no conflict	no conflict	no conflict	camera conflict - queue	motor conflict - reject new & prevent	danger - kill current, reject new & prevent	no conflict	no conflict	danger - kill current, reject new & prevent
	x	18	Mini-TES	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	motor conflict - reject new	no conflict	payload conflict - queue	payload conflict - queue	no conflict
		19	point/home mast	no conflict	no conflict	no conflict	no conflict	no conflict	no conflict	motor conflict - reject new	no conflict	no conflict	no conflict	no conflict
x		20	any camera image	no conflict	camera conflict - queue	no conflict	no conflict	no conflict	camera conflict - queue	no conflict	no conflict	no conflict	no conflict	no conflict
x		21	point & shoot with Pancam or Navcams	no conflict	camera conflict - queue	no conflict	no conflict	no conflict	camera conflict - queue	motor conflict - reject new	no conflict	no conflict	no conflict	no conflict
		22	shutdown now	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new
		23	battery going offline response	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new
		24	web overtemperature response	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new
x		25	diagnostic imagining using navcams & hazcams response	no conflict	camera conflict - queue	no conflict	no conflict	no conflict	camera conflict - queue	motor conflict - kill current & prevent future, service new	no conflict	no conflict	no conflict	no conflict

Surface Ops Behavior Relationships Matrix (continued)

"A" is active and "B" is requested			camera	x			x	x				x
			payload interface		x							
				17	18	19	20	21	22	23	24	25
			"B" Behaviors / behavior category / "A" Behaviors	coordinated Microscopic Imager & arm use	Mini-TES	point/home mast	any camera image	point & shoot with Pancam or Navcams	shutdown now	battery going offline response	web overtemperature response	diagnostic imagining using navcams & hazcams response
		2	LGA DTE communication	no conflict	no conflict	no conflict	no conflict	no conflict	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	no conflict
x		4	attitude acquisition/update for HGA communications	camera conflict - queue	no conflict	no conflict	camera conflict - queue	camera conflict - queue	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	camera conflict - queue
		5	HGA DTE communication	no conflict	no conflict	no conflict	no conflict	no conflict	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	no conflict
		6	UHF communications	no conflict	no conflict	no conflict	no conflict	no conflict	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	no conflict
		7	stow SHAG/ pre-load for drive	no conflict	no conflict	no conflict	no conflict	no conflict	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	no conflict
x		8	attitude acquisition/update for mobility and science	camera conflict - queue	no conflict	no conflict	camera conflict - queue	camera conflict - queue	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	camera conflict - queue
x		10	any rover drive or steer cmd	motor conflict - reject new & prevent	motor conflict - reject new & prevent	motor conflict - reject new & prevent	camera conflict - queue	motor conflict - reject new & prevent	intent conflict - reject new & prevent	intent conflict - reject new & prevent	intent conflict - reject new & prevent	motor conflict - complete, then service new
		11	position/stow arm	danger - kill current, reject new & prevent	no conflict	no conflict	no conflict	no conflict	intent conflict - reject new & prevent	intent conflict - reject new & prevent	intent conflict - reject new & prevent	no conflict
	x	12	any Mössbauer Spectrometer commanding & data transfer	no conflict	payload conflict - queue	no conflict	no conflict	no conflict	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	no conflict
	x	14	any APXS commanding & data transfer	no conflict	payload conflict - queue	no conflict	no conflict	no conflict	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	no conflict
		16	RAT (expose surface)	danger - kill current, reject new & prevent	no conflict	no conflict	no conflict	no conflict	intent conflict - reject new & prevent	intent conflict - reject new & prevent	intent conflict - reject new & prevent	no conflict
x		17	coordinated Microscopic Imager & arm use	danger - kill current, reject new & prevent	no conflict	no conflict	camera conflict - queue	camera conflict - queue	intent conflict - reject new & prevent	intent conflict - reject new & prevent	intent conflict - reject new & prevent	camera conflict - queue
	x	18	Mini-TES	no conflict	payload conflict - queue	mast conflict - complete, then service new	no conflict	mast conflict - complete, then service new	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	mast conflict - complete, then service new
		19	point/home mast	no conflict	mast conflict - complete, then service new	mast conflict - complete, then service new	no conflict	mast conflict - complete, then service new	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	mast conflict - complete, then service new
x		20	any camera image	camera conflict - queue	no conflict	no conflict	camera conflict - queue	camera conflict - queue	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	camera conflict - queue
x		21	point & shoot with Pancam or Navcams	camera conflict - queue	mast conflict - complete, then service new	mast conflict - complete, then service new	camera conflict - queue	mast conflict - queue	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	mast conflict - queue
		22	shutdown now	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - reject new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new
		23	battery going offline response	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - reject new	intent conflict - reject new	intent conflict - kill current & service new	intent conflict - kill current & service new
		24	web overtemperature response	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - kill current & service new	intent conflict - reject new	intent conflict - reject new	intent conflict - reject new	intent conflict - kill current & service new
x		25	diagnostic imagining using navcams & hazcams response	camera conflict - queue	mast conflict - complete, then service new	mast conflict - complete, then service new	camera conflict - queue	mast conflict - kill current & service new	intent conflict - reject new	do offline resp, reject new	intent conflict - reject new	intent conflict - reject new

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-12-2005	Contractor's Report	May 2005-October 2005

4. TITLE AND SUBTITLE

Preliminary Report on Mission Design and Operations for Critical Events

5a. CONTRACT NUMBER
NNA04AA18B

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
21-103-06-40-1

6. AUTHOR(S)

Sandra C. Hayden
Irem Tumer

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Ames Research Center
Moffett Field, CA 94035-1000

8. PERFORMING ORGANIZATION REPORT NUMBER

NASA/CR-2005-213472

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITOR'S ACRONYM(S)
NASA

11. SPONSORING/MONITORING REPORT NUMBER

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified -- Unlimited
Subject Category 12 Distribution: Standard
Availability: NASA CASI (301) 621-0390

13. SUPPLEMENTARY NOTES
Point of Contact: Sandra Hayden, NASA Ames Research Center, MS 269-3, Moffett Field, CA 94035-1000 (650) 604-1676

14. ABSTRACT

Mission-critical events are defined in the Jet Propulsion Laboratory's Flight Project Practices as those sequences of events which must succeed in order to attain mission goals. These are dependent on the particular operational concept and design reference mission, and are especially important when committing to irreversible events. Critical events include main engine cutoff (MECO) after launch; engine cutoff or parachute deployment on entry, descent, and landing (EDL); orbital insertion; separation of payload from vehicle or separation of booster segments; maintenance of pointing accuracy for power and communication; and deployment of solar arrays and communication antennas. The purpose of this paper is to report on the current practices in handling mission-critical events in design and operations at major NASA spaceflight centers. The scope of this report includes NASA Johnson Space Center (JSC), NASA Goddard Space Flight Center (GSFC), and NASA Jet Propulsion Laboratory (JPL), with staff at each center consulted on their current practices, processes, and procedures.

15. SUBJECT TERMS
critical events, mission design, mission operations, standards, mishaps, International Space Station rendezvous and docking, Mars Exploration Rover surface operations, remote sensing, satellite operations

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	50	