



**2004 SpaceOps Conference
Montreal, Canada, 17-21 May 2004**

**MANAGING RISK TO ENSURE A
SUCCESSFUL CASSINI/HUYGENS
SATURN ORBIT INSERTION (SOI)**
(Paper by: Mona M. Witkowski, Shin M. Huh, John B. Burt & Julie
L. Webster)

**Presented by
Mona M. Witkowski
19 May 2004**



Agenda

- Introduction
- Distributed Operations
- Cassini Risk Management Implementation
- SOI Risk Management
- SOI Risk Identification & Mitigation
- Independent Assessment
- In-Flight Validation Activities
- SOI Communication Strategy
- Mission Assurance Risk Assessment
- Summary

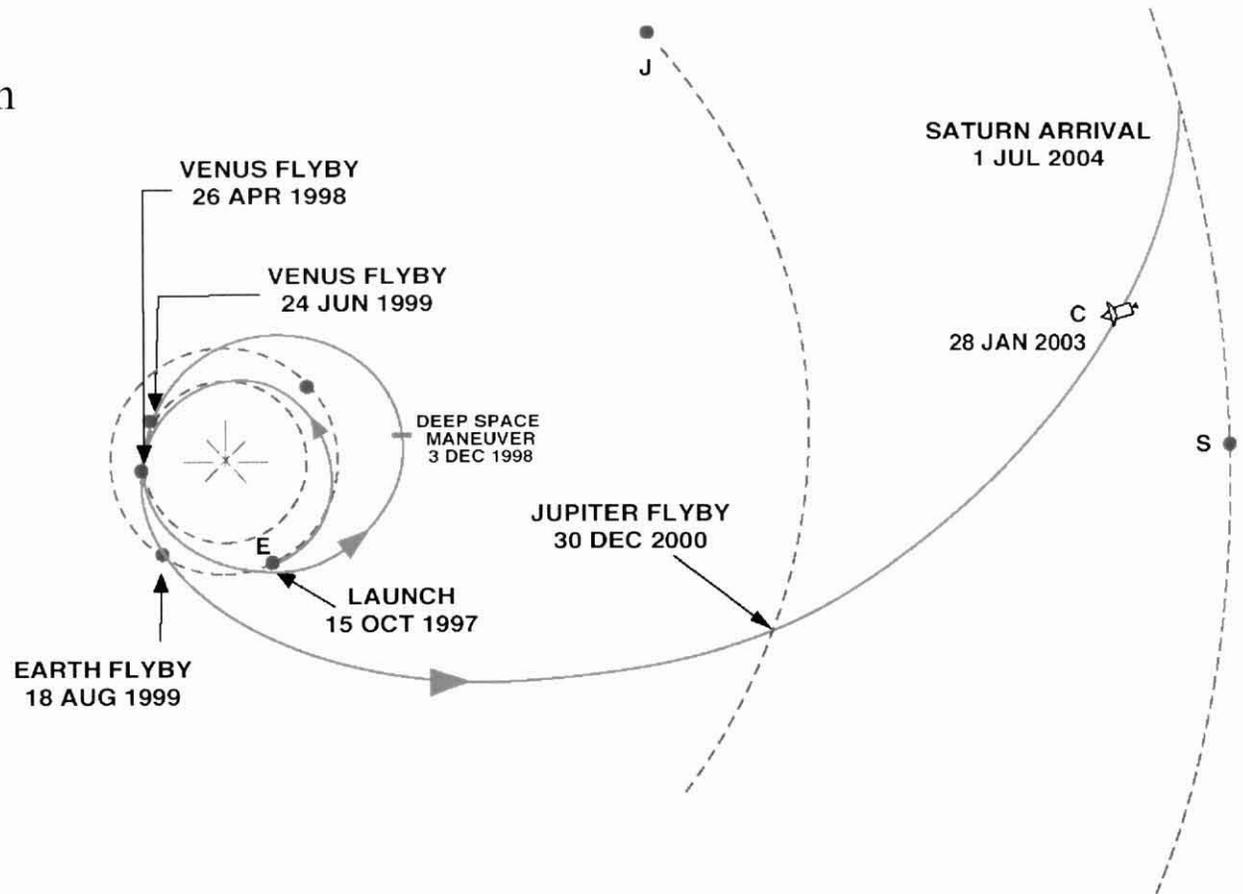
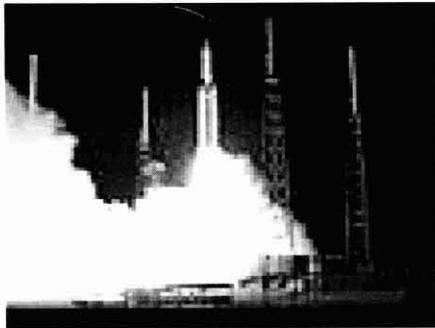


Introduction

CASSINI MISSION CRUISE TRAJECTORY

Earth (E), Jupiter (J), Saturn (S), and Cassini (C) locations on 28 January 2003

- Cassini/Huygens is a joint NASA/ESA mission to Saturn
- Launched October 15, 1997



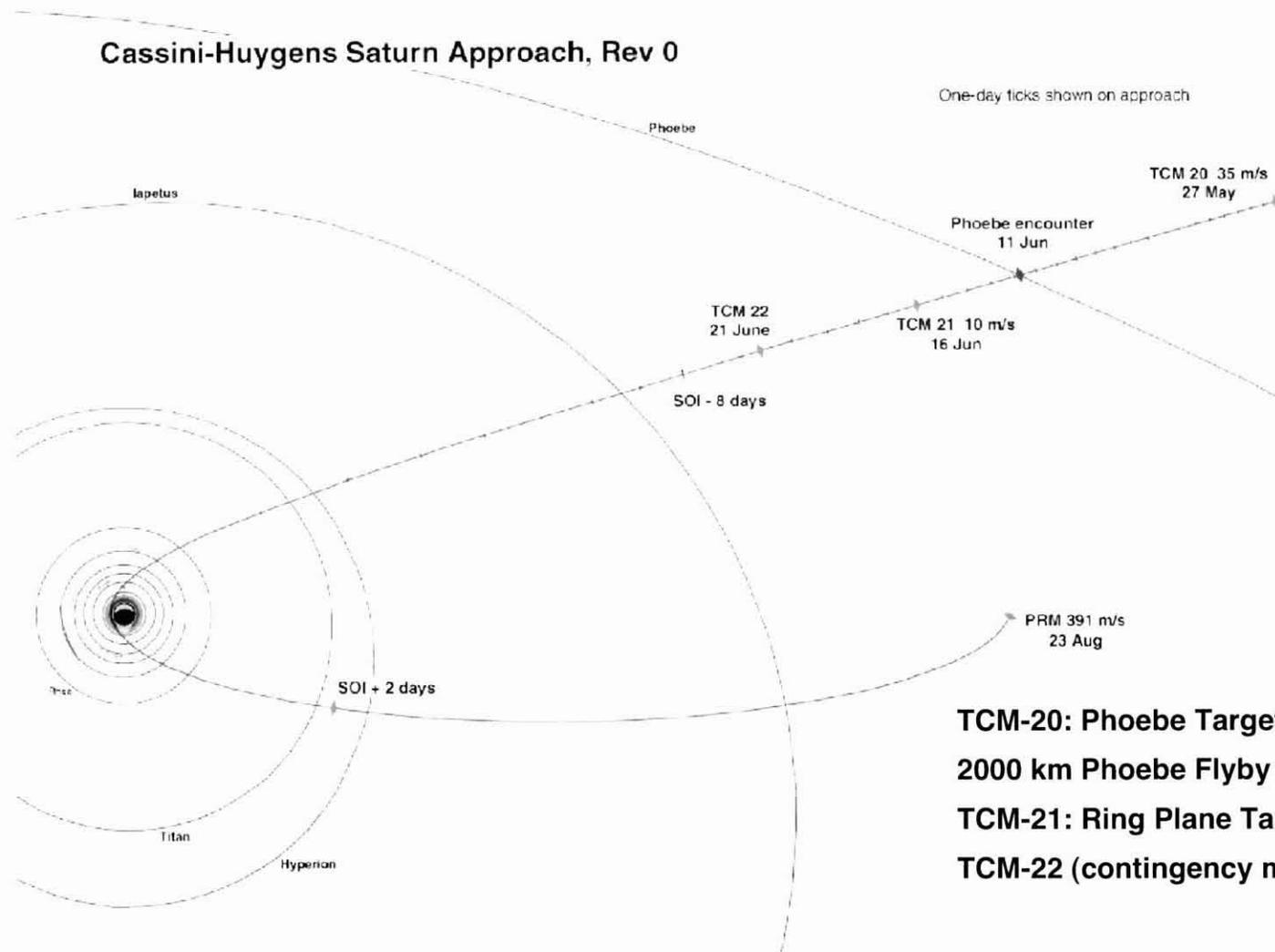
- Saturn Orbit Insertion (SOI)
 - July 1, 2004 01:12 UTC
- Probe release at Titan 12/04
 - Probe Relay 1/14/05



Introduction

(Continued)

Cassini-Huygens Saturn Approach, Rev 0



- TCM-20: Phoebe Targeting Maneuver**
- 2000 km Phoebe Flyby**
- TCM-21: Ring Plane Targeting**
- TCM-22 (contingency maneuver)**

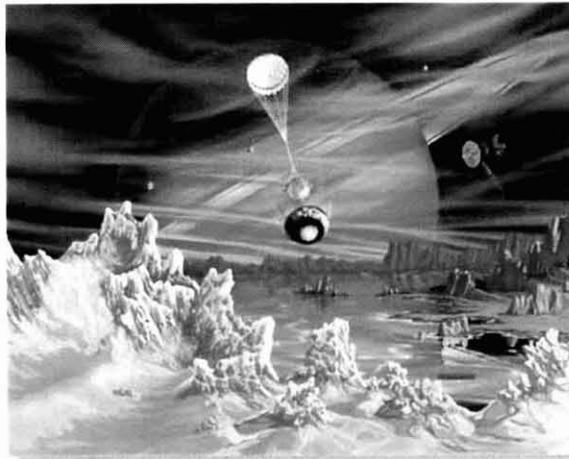
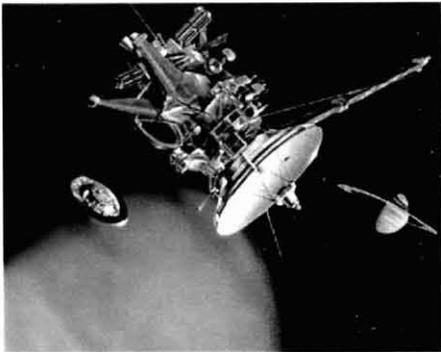
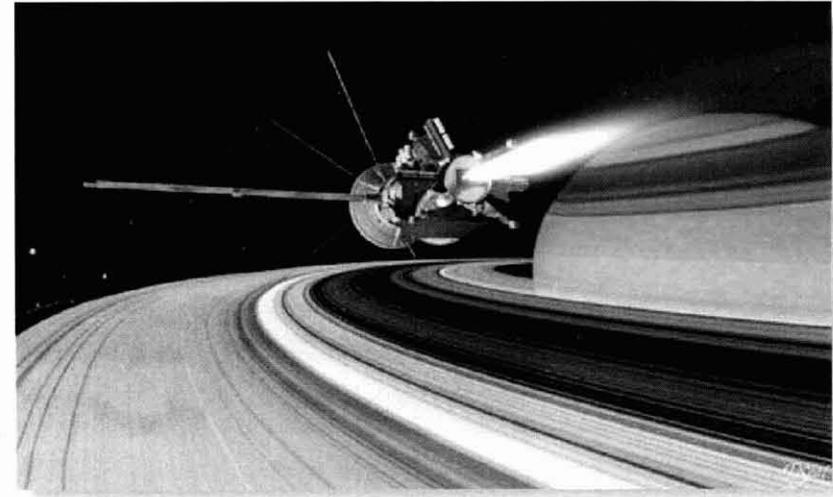


Introduction

(Continued)

Saturn Orbit Insertion (SOI)

- SOI Burn - July 1, 2004 @ 01:12 UTC
- Burn Duration - 96.4 min
- Nominal ΔV : 626 m/s
- Ring Plan Crossings
 - Ascending @ 00:47 UTC
 - Descending @ 04:34 UTC
- Critical Mission Event - Failure is not an option
- Essential for Probe Mission & Tour Operations

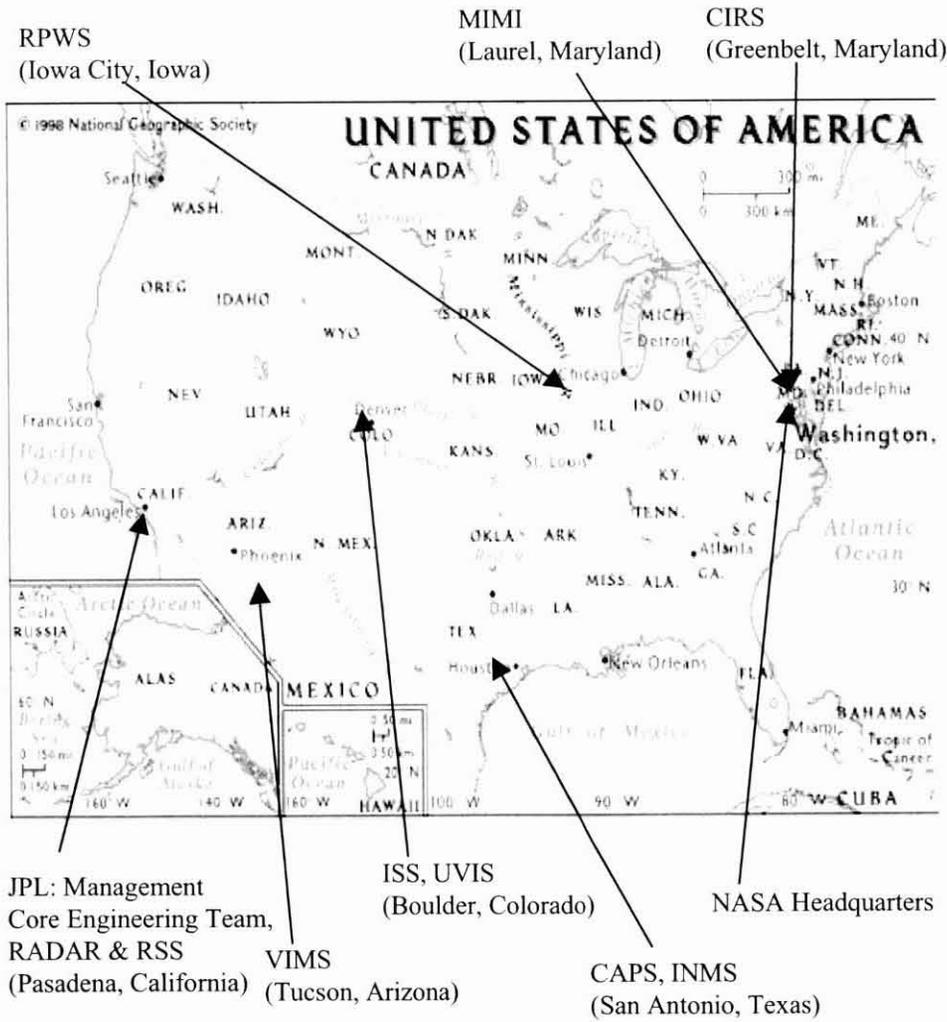


Huygen's Probe Mission

- Probe Release - December 4, 2004
- Probe Relay - January 14, 2005



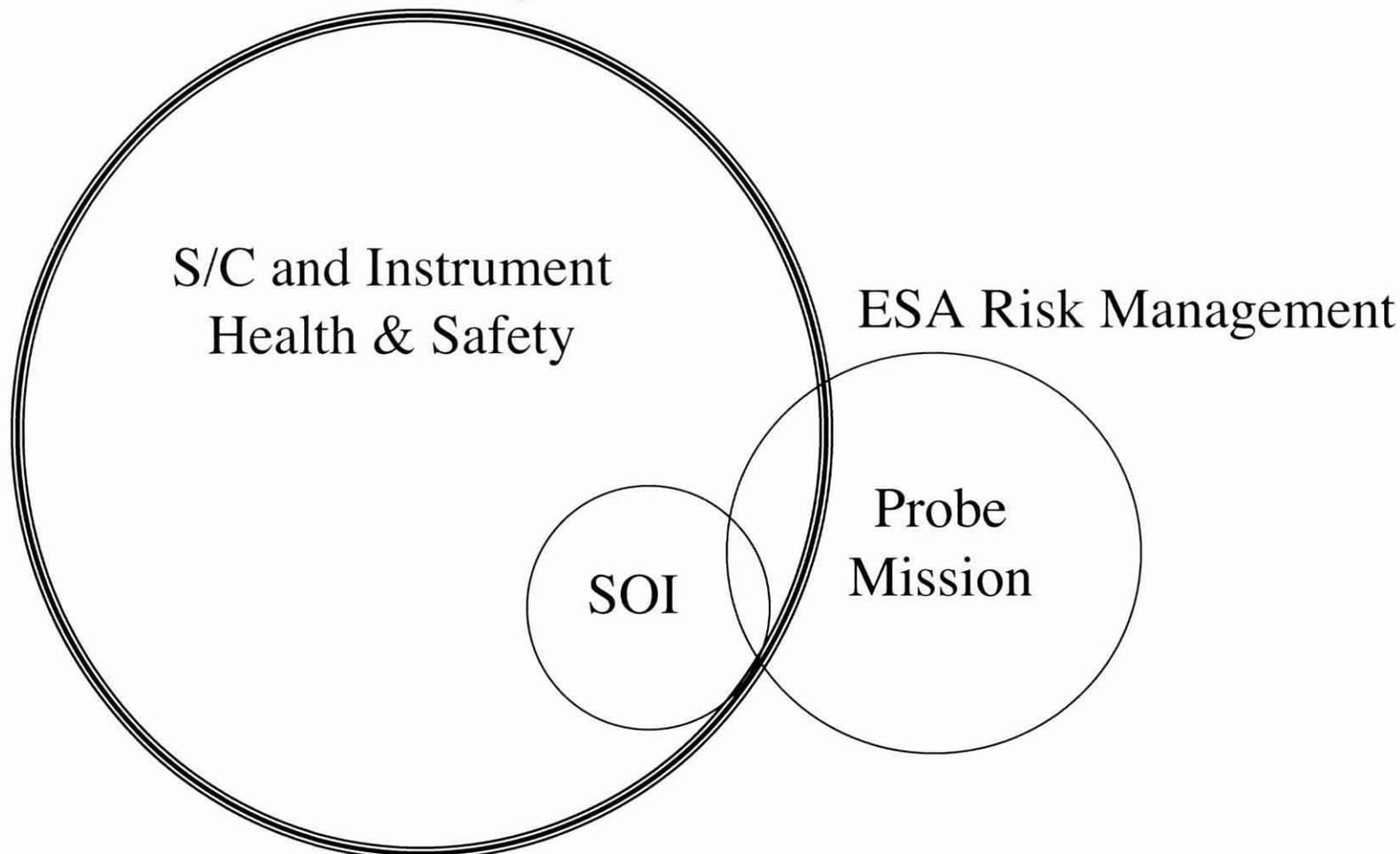
Distributed Mission Operations





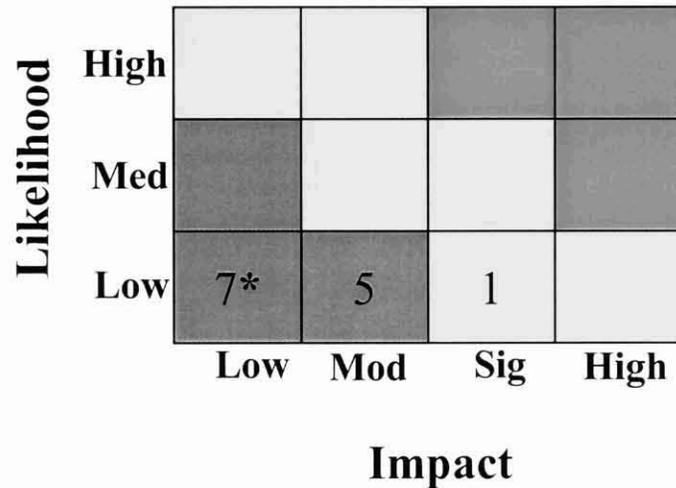
Cassini Risk Management Implementation

JPL Risk Management





SOI Risk Management



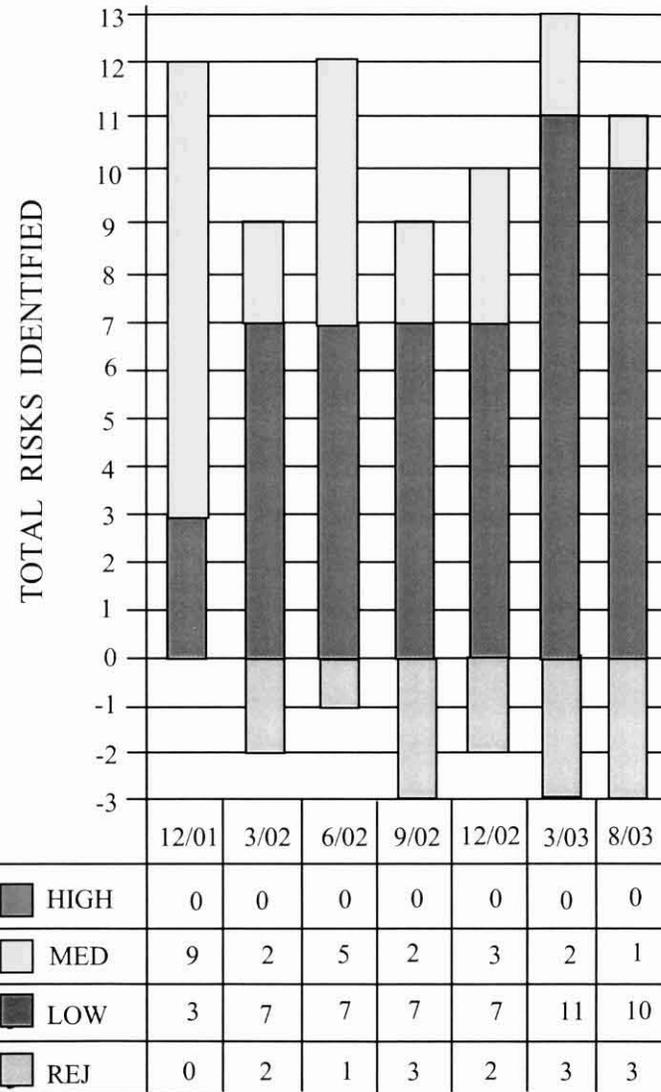
LIKELIHOOD

- High** Risk Event is likely to occur ($\geq 10\%$ probability)
- Med** Risk Event may occur ($< 10\%$ probability)
- Low** Risk Event is unlikely to occur ($< 1\%$ probability)

IMPACT

- High** Impact not repairable within allocated resources
- Sig** Impact may not be repairable within allocated resources
- Mod** Impact may be repairable within allocated resources
- Low** Impact of occurrence easily repairable within allocated resources

* 2 retired risks are not included in the metrics.





SOI Risk Management

(Continued)

Design

- S/C designed to be largely single fault tolerant
- Operate in flight demonstrated envelope, with margin
- Strict compliance with requirements & flight rules

Test

- Baseline, fault & stress testing using flight system testbeds (H/W & S/W)
- In-flight checkout & demos to remove first time events

Failure Analysis

- Critical event driven fault tree analysis
- Risk mitigation & development of contingencies

Residual Risks

- Accepted pre-launch waivers to Single Point Failures
- Unavoidable risks (e.g. natural disaster)

Mission Assurance

- Strict process for characterization of variances (ISAs, PFRs & Waivers)
- Full time Mission Assurance Manager reports to Program Manager
 - Independent assessment of compliance with institutional standards
 - Oversight & risk assessment of ISAs, PFRs & Waivers etc.
 - Risk Management Process facilitator



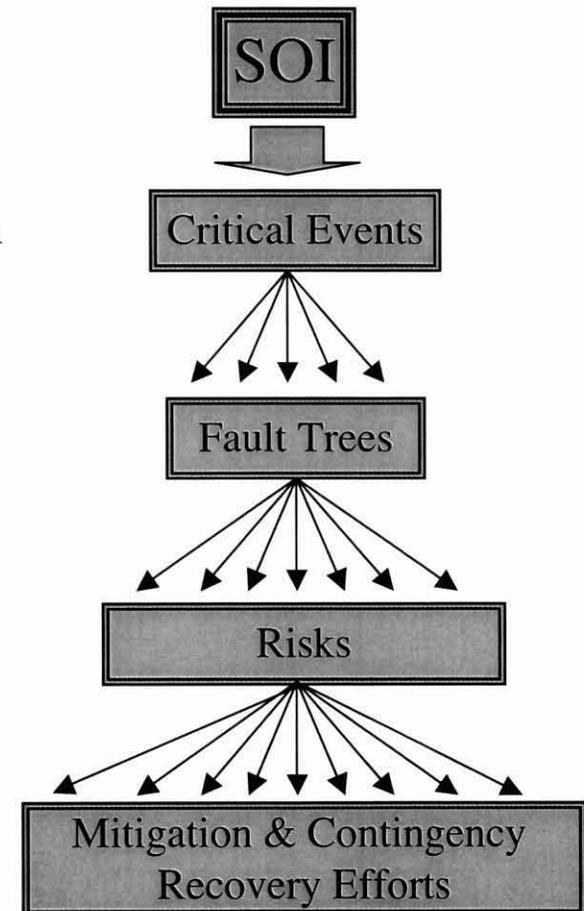
Risk Identification & Mitigation

Pre Launch

- Prelaunch Risk Management Process
- FMECAs used extensively
 - S/C designed to be single fault tolerant
 - Limited Single Point Failures (SPF) waived prelaunch

Post Launch

- Continued Flight S/W development & test
 - Extensive FSW & fault protection upgrades
- SOI Critical Sequence development, analysis & test
 - 2 additional SPFs identified & S/W mods to mitigate
- Top down fault tree / event tree analysis
 - Critical Events & potential faults identified
 - Mitigation efforts and contingencies developed
- Detailed risks and mitigation efforts documented
 - Mission risks in programmatic Sig Risk List (SRL)
 - Off nominal fault tree results captured
 - Additional ground response / contingency plans developed

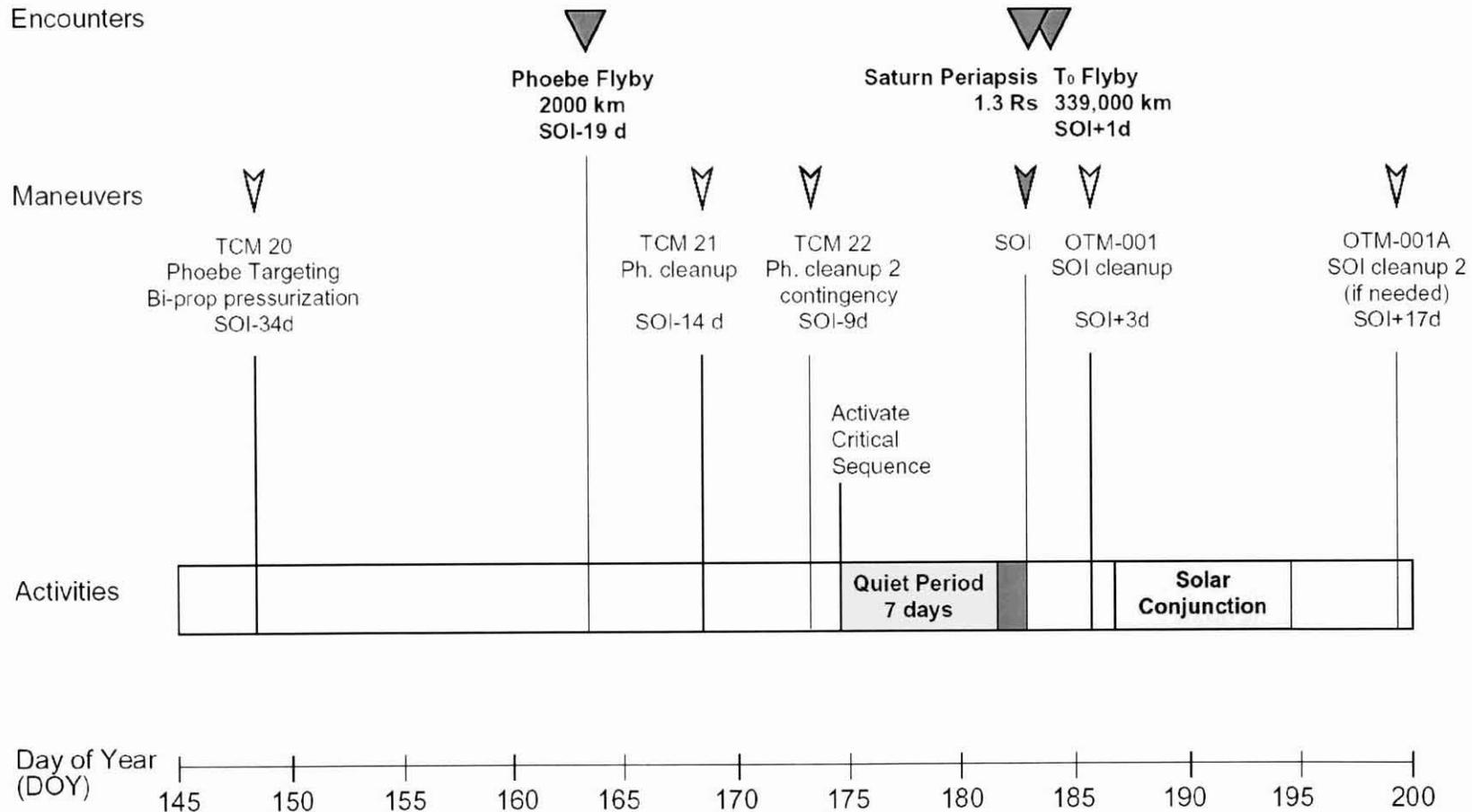




Risk Identification & Mitigation

(Continued)

SOI Events Timeline

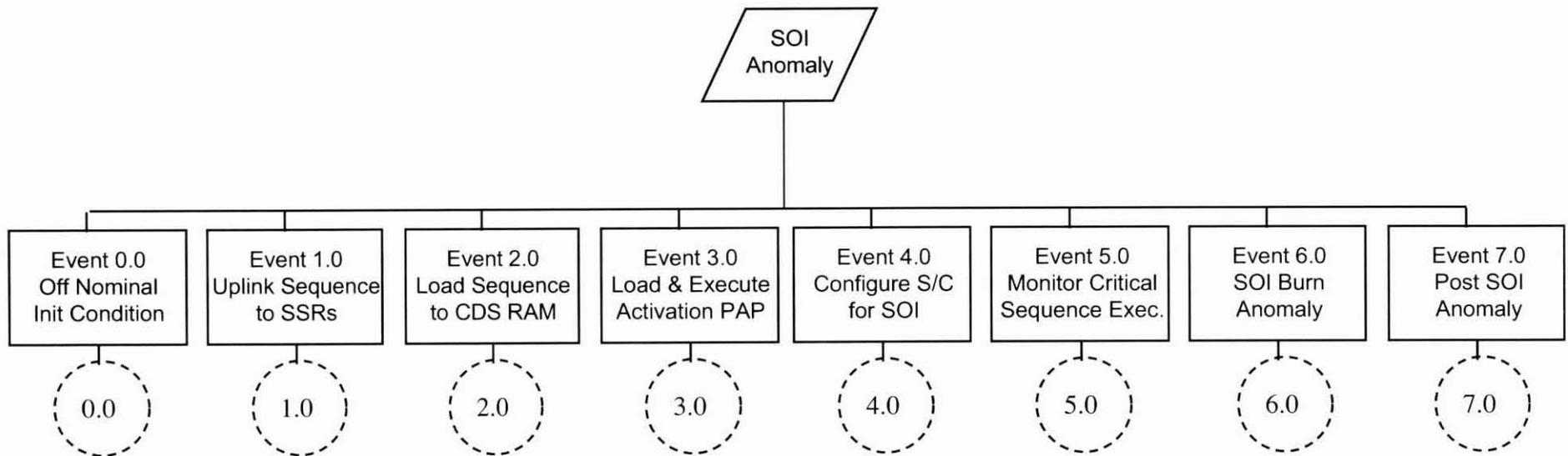




Risk Identification & Mitigation

(Continued)

SOI Event Critical Event / Timeline

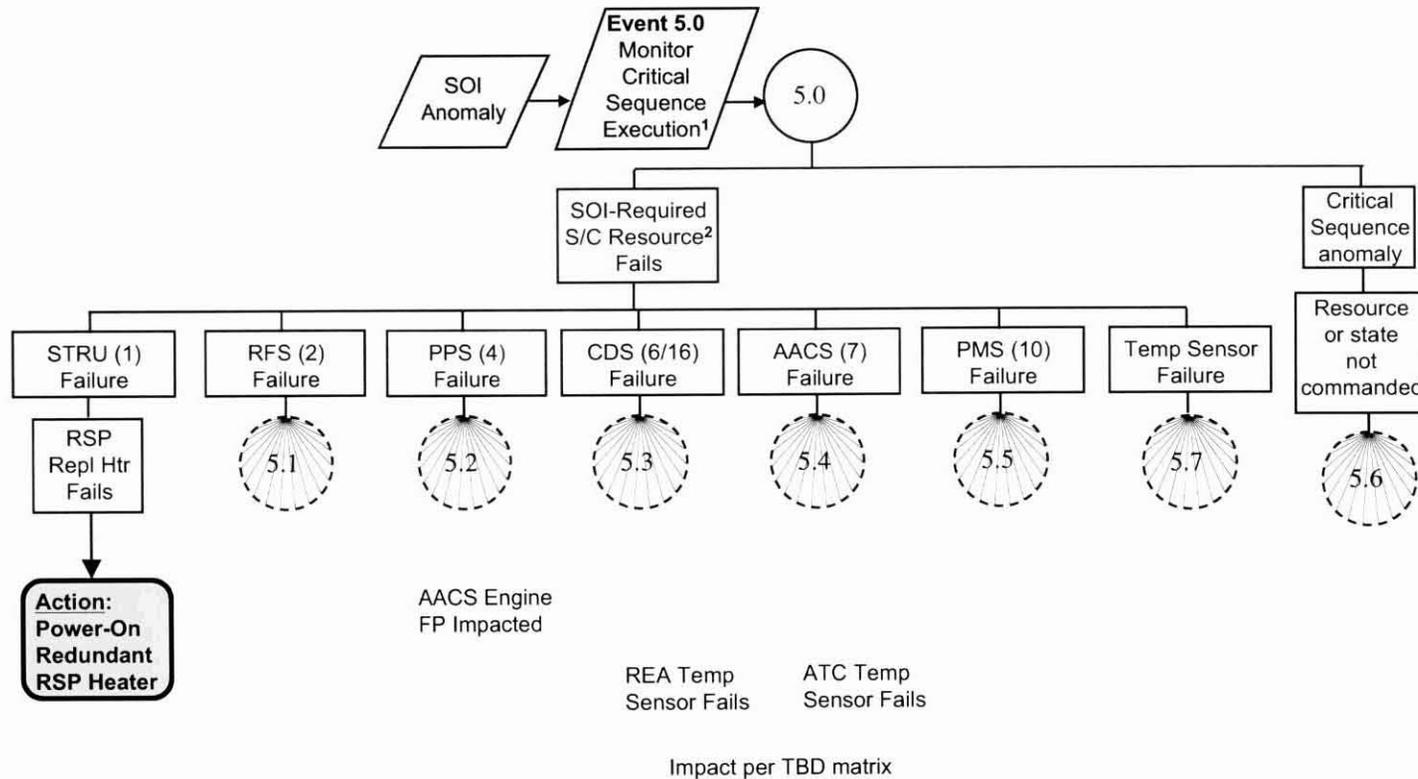




Risk Identification & Mitigation

(Continued)

SOI/Event 5.0 Fault Tree



¹ Last Opportunity (LO) for Ground Contingency U/L = (LGA-1 Swap) - (OWLT)

² Resources NOT required include: Probe, Instruments, RWAs, Bail

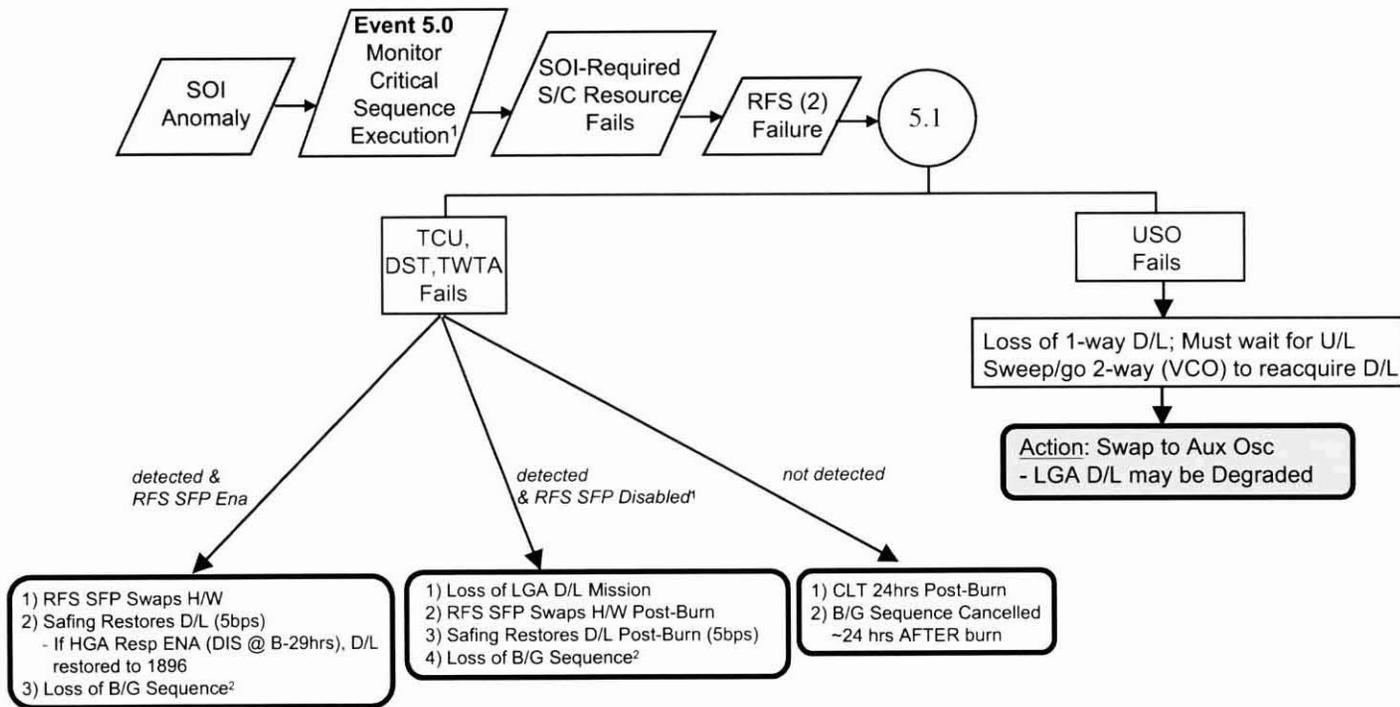
Note: Fault Trees have implicit 'logical OR' at each branch



Risk Identification & Mitigation

(Continued)

SOI/Event 5.1 Fault Tree



Note: Fault Trees have implicit 'logical OR' at each branch

¹ RFS SFP is disabled from 03:40 hrs prior to Swap to LGA-1/Turn to ARPC Attitude until after the end of the burn.
² The loss of the B/G seq will require R/T configuration before burn or post-burn action req'd to cleanup/prepare for OTM-1.



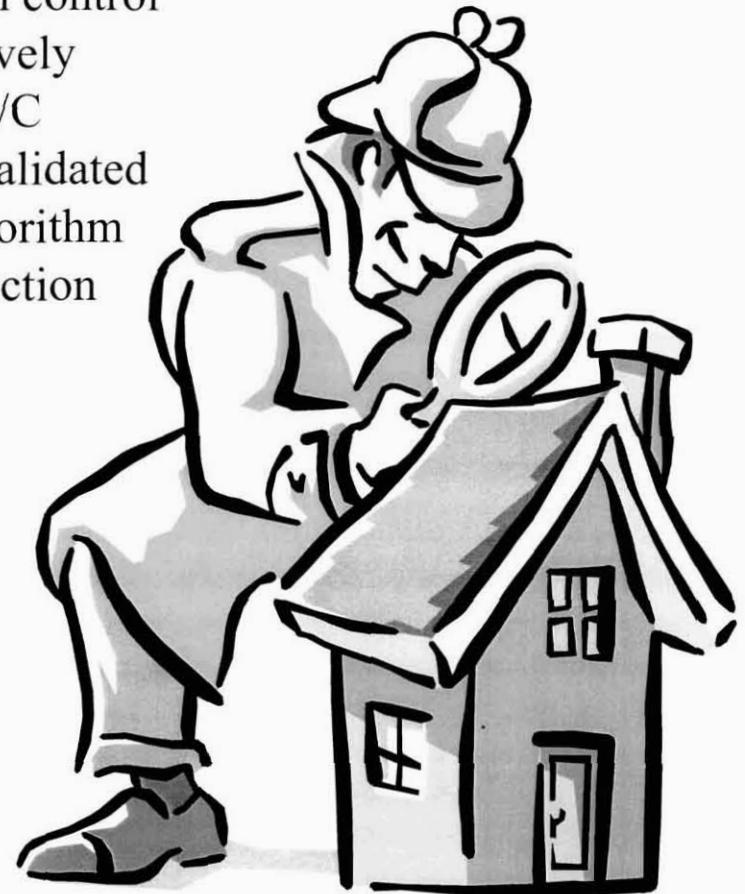
Independent Assessment

Extensive Peer Reviews and Testing

- Peer Reviews preceded every major Design/Risk Review
- SOI Critical Sequence is under strict configuration control
- The sequence has been tested and retested extensively
- Additional validation performed in-flight on the S/C
- Critical Events and Fault Scenarios identified & validated
- Addition & validation of AACCS “Smartburn” Algorithm
- Flight Software changes for additional Fault Protection

Independent Reviews

- SOI Preliminary Design Review - October 2000
- Critical Sequence Design/Risk Review - February 2002
- “Smartburn” Flight Software Algorithm Review -
- SOI Risk Review - October 2003
- SOI Critical Events Readiness Review - April 2004





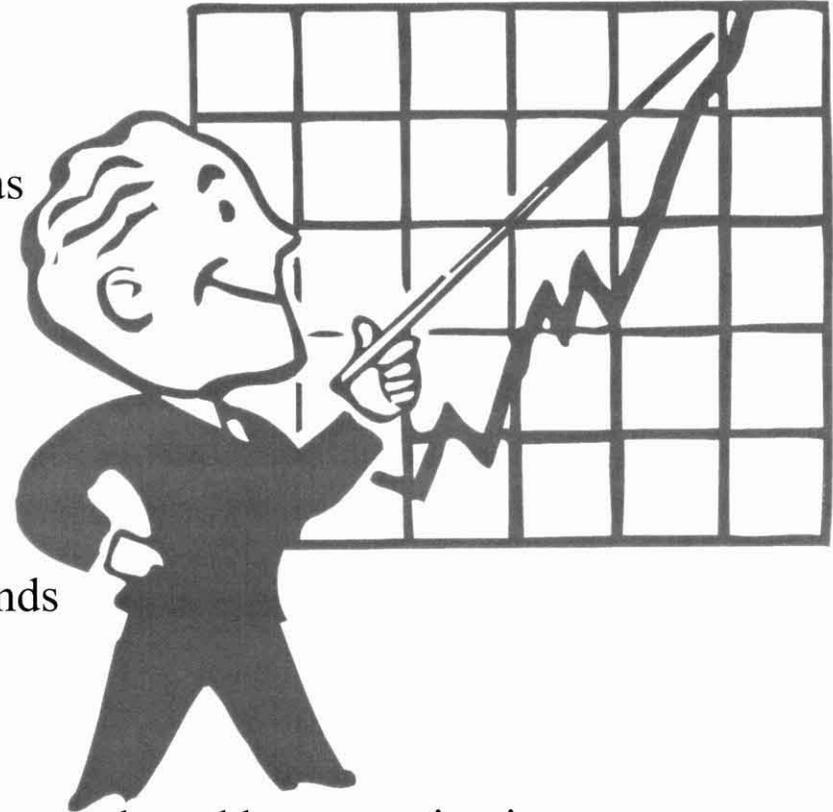
In-Flight Validation Activities

First Time Events

- First time events identified as potential risk areas
- Mitigated risk by demonstrating in-flight

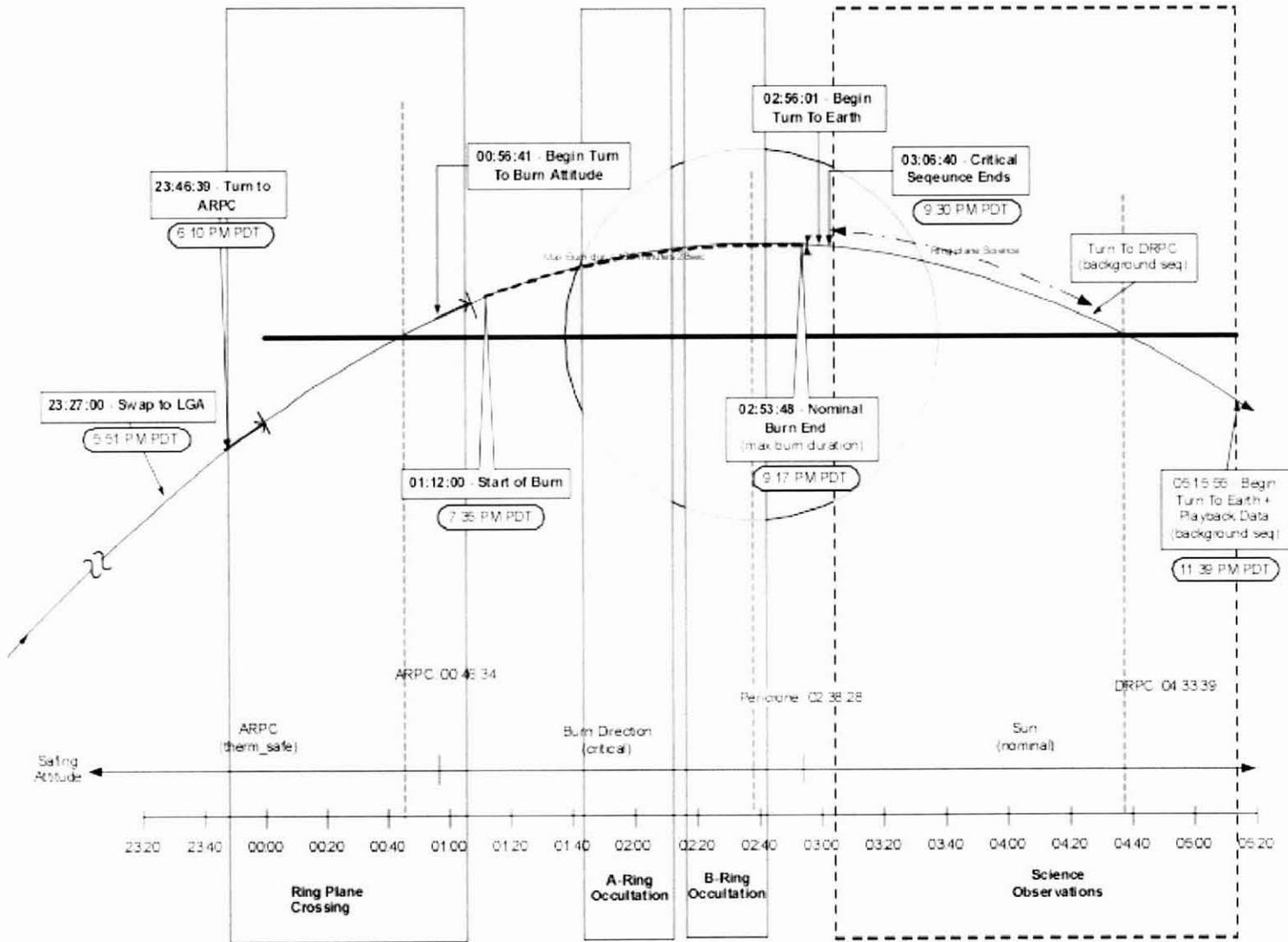
In Flight Verification

- SOI Critical Sequence Demonstration
 - July 2003
- TCM-19 - May 2003
 - Main Engine (ME) cover closure at 126 seconds
 - Use of both ME engines simultaneously
 - Verified heater usage after end of burn
- TCM-19b - November 2003
 - Validation of “Smartburn” Algorithm, with energy based burn termination
- TCM-20 - May 2004
 - First burn on SOI AACS Flight Software Load (A8.6.6)
 - First long burn with MAG boom deployed





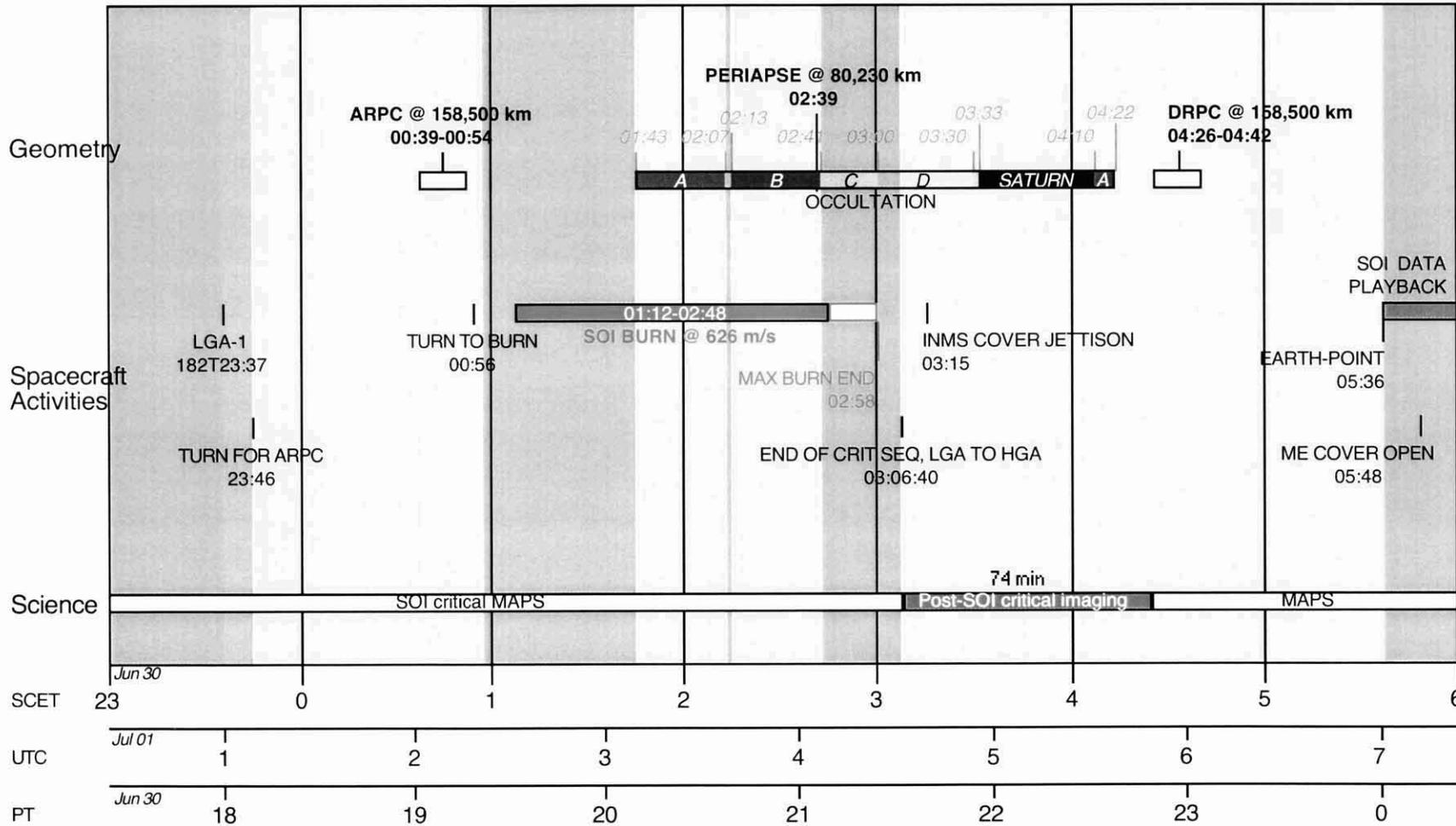
SOI Turn & Communication Strategy





Communication Strategy

□ No comm □ Comm, carrier only □ Comm + telemetry



Hour of Day for DOY 182-183 (30 Jun - 01 Jul 2004)



Mission Assurance Risk Assessment

- **The Cassini Team is engaged in Risk Management**
- **Risks to SOI have been proactively identified & mitigated**
 - **Event Trees generated & mapped to Contingency Plans**
 - **Critical Event Timeline analyzed for dependencies & downstream failure impacts**
 - **Programmatic Risks Mitigated**
 - **No residual risk from Red Flag Failure Reports**
- **The SOI Critical Sequence has undergone rigorous testing**
 - **Numerous nominal and fault conditions simulated**
- **Final versions of AACCS & CDS Flight Software are onboard**
- **No Risks to achieving a successful SOI have been identified from a Mission Assurance perspective**



Summary

- **SOI Risk Management has been a disciplined, well thought out effort**
- **Cassini Flight Team embraces Risk Management**
- **SOI must be Successful - Failure is not an option**
- **SOI Risks are identified/mitigated from the top down & bottoms up (programmatic RM / Fault Trees / FMECAs)**
- **Cassini is ready for Saturn Orbit Insertion**



Backup



Existing Risks and Mitigation Efforts

Open Risks:

Low/Low

35 - S/C Fault is detected prior to SOI

Mitigation: Mitigated by disabling system level fault protection that is not necessary to achieving SOI. The SOI sequence is loaded onboard the S/C eight days prior to SOI & the S/C is placed into a quiescent state.

Low/Low

36 - Loss of downlink prior to SOI

Mitigation: A loss of D/L caused by the ground will have no effect on the S/C, once the SOI sequence is enabled (8 days prior to SOI). Loss of D/L caused by the S/C will be handled by onboard systems and AACS fault protection routines.

Low/Low

37 - Loss of commandability prior to SOI

Mitigation: Conservative command loss timer management & double station coverage is provided during SOI. Contingency plans & procedures are in place.

Low/Low

39 - Loss of primary pressure regulator prior to SOI

Mitigation: Failure of the prime pressure regulator at SOI has been waived as a single point failure (#84465 & 84526). The primary pressure regulator will be checked out during TCM-20 and the Phoebe targeting maneuver, which has been designed as a regulated maneuver to characterized regulator performance. Contingency plans & procedures are in place.



Existing Risks and Mitigation Efforts

(Continued)

Open Risks:

Low/Mod

40 - Main engine cover sticks in place, either open, closed or in between

Mitigation: The main engine cover will be opened and verified to be retracted for TCM-20 and the Phoebe targeting maneuver. It will be left open for SOI. If the cover can not be opened enough to be able to perform an main engine burn, pyro devices are available to separate the cover from the S/C. With two drive motors for the cover, a double failure would have to occur before cover ejection would be considered. Contingency plans & procedures are in place.

Low/Mod

41 - Failure to communicate with the S/C after SOI

Mitigation: The SOI critical sequence ends with the S/C at Earth point. Any recoverable fault that occurs during SOI will be dealt with and the S/C will return to Earth point. The command loss timer will be down to ~24 hours at the conclusion of SOI. In the event that we are unable to communicate with the S/C following SOI, Uplink Loss System Fault Protection would begin executing ~24 hours later. There would be multiple opportunities to recover the S/C. This could possibly affect the size and timing of OTM-1, but not the overall mission objectives. Contingency plans and procedures are in place.



Existing Risks and Mitigation Efforts

(Continued)

Open Risks:

Low/Sig

43 - Partial execution of SOI could impact mission objectives by deviating from the planned tour trajectory

Mitigation: There is sufficient time in the SOI maneuver to have multiple burns and burn restarts on the two engines. An energy based delta V algorithm was added in January 2002, for added robustness of the design and to allow for delayed first burn starts. Between the existing fault protection and this added design, it would take multiple faults (>2) AACS faults to have the possibility of achieving only a partial SOI execution.

Low/Mod

45 - Large SOI Navigation Errors

Mitigation: Large Navigation errors are certainly a possibility, however flight experience to date has resolved deviations down to mm/sec. During 12 TCMs (through 3/02), uncertainties have been below one sigma. In addition, Optical Navigation capabilities are now on-board (5/03) the spacecraft and provide an independent check of any navigation errors.

Low/Mod

46 - Loss of a main engine during SOI

Mitigation: A second main engine was added early in the design phase because there was enough time to try a second burn and still achieve SOI. SOI is a critical sequence that has fault protection in place to swap to the backup engine in the event of a failure or underperformance of the primary engine.



Existing Risks and Mitigation Efforts

(Continued)

Open Risks:

Low/Mod

106 - Anomalous PMS pressurization/TCM-20

Mitigation: The pyro un-isolation activities are done in time to have multiple chances to fix any problems. A fault analysis tree has been done & contingency commands are in place. All other events leading up to the actual pressurization are done in time for ground-in-the-loop intervention if necessary. The actual opening of LV 10 to pressurize the PMS bi-prop system is done just prior to TCM-20 burn to minimize fault conditions for LV 10. Should LV 10 not open up, TCM-20 can execute just fine in blowdown mode, and the ground will deal with the LV 10 failure.

Low/Low

107 - An anomalous or missed TCM-21

Mitigation: TCM-21 is currently only a placeholder for a TCM-20 cleanup maneuver. There is also an opportunity for a TCM-22 if needed.

Low/Low

113 - Sun Sensor article impact

Mitigation: There are several mitigation options available: 1) Alternative S/C Attitudes - Fly Main Engine to RAM (cover designed to protect) - Other regions to RAM 2) Alternative Attitude Knowledge capability - Flight Software Mod (Deluxe AI) to use star tracker 3) Further Analysis - Probabilistic Risk Assessment of sun sensor particle impact.



Existing Risks and Mitigation Efforts

(Continued)

Open Risks:

Low/Low

114 - Reloading AFC at SOI - 2 Months

Mitigation: The parameter update procedures will be detailed, reviewed and thoroughly tested on the ground (in ITL) prior to execution on the spacecraft. AFC reloads have been accomplished successfully several times in flight, with the last one being performed for the AACS V8.6.5 FSW uplink & checkout in February 2003.

Retired Risks:

Low/Low

64 - AACS FSW V8 Criticality

Mitigation: Uplink and checkout of the FSW occurred in February 2003. This risk was retired following successful execution of the SOI demo in July 2003.

Low/Mod

65 - CDS FSW V9 Criticality

Mitigation: The FSW was uplinked in February 2003 and completed a rigorous checkout on April 30, 2003. This risk was retired upon successful execution of the SOI demo in July 2003.



Existing Risks and Mitigation Efforts

(Continued)

Rejected Risks:

38 - SOI Failure

Rationale: Complete failure would result in the end of mission. This risk is addressed and encompassed in all of the other SOI related risks.

42 - Failure of S/C to survive SOI

Rationale: Complete failure would result in the end of mission. This risk is addressed and encompassed in all of the other SOI related risks.

44 - Particle Impact Interferes with SOI

Rationale: This risk is addressed and encompassed under the Mission Planning particle impact risk statements.



Single Point Failures

• SPF Exemptions

1. Loss of a Radioisotope Thermoelectric Generator (RTG)
2. Loss of High Gain Antenna (HGA) or either Low Gain Antenna inside 1.5 AU
3. Leakage or bursting of a propulsion module tank (pressurant tank, main engine oxidizer tank, main engine fuel tank, thruster hydrazine tank)
4. Leakage or bursting of propulsion module fluid or pressurant lines and fittings
5. Structure (Spacecraft, adapter, orbiter or Probe truss)
6. Spacecraft separation band (retention / release)
7. Thermal blankets, surfaces and shields (Spacecraft & Probe)
8. Spacecraft cabling short, trace short or open on PWBs (does not include VIAs)
9. Selected command and data errors
10. Main Engine combustion chamber (catastrophic explosion)
11. Passive radio frequency equipment (3dB hybrid)
12. Micrometeoroid shielding (inherent or specific)
13. Power interruption greater than 37 Msec
- 14-18. Probe adapter structures, Probe Structure, spin-up and release mechanisms (exemption not applicable to premature release), heat shield, parachute systems

*** Reference: 699-004 Project Policies and Requirements & Cassini Risk Assessment Review, Single Point Failure, C.P. Jones, 08/18/97**



Single Point Failures

(Continued)

- **Approved SPF Waivers**

- **84373: PMS #F1 He Filter** - Allows a single main helium system filter (F1).

Risk: Low. Filter size doubled, resulting factor of safety is 18.4. LMA implemented stringent tank cleaning requirements.

- **84745: PMS #F2 Filter During SOI** - The failure of F2 during SOI, by either partial or total clogging, represents a SPF.

Risk: Negligible. Conservative sizing of the F2 filter & stringent cleaning requirements.

- **84465: PMS Regulator Fail Closed During SOI** - Failure of one of the regulators in the closed position during SOI (whichever regulator is active for SOI) represents a SPF.

Risk: Negligible. Principal failure mode is relevant to the regulators with a soft seat which potentially can extrude and result in a stuck closed regulator. The Cassini regulator is a hard seat regulator and the FMECA concluded this failure mechanism is either non-credible or highly unlikely.

* **Reference: Cassini Risk Assessment Review, Single Point Failure, C.P. Jones, 08/18/97**



Single Point Failures

(Continued)

- **Approved SPF Waivers**

- **84526: PMS Overpressure at SOI** - It is planned to disable the overpressure fault protection at a safe time prior to SOI.

Risk: Low. System will have been previously pressurized and regulator lock-up verified.

- **84896: Soft Shorts** - A “soft” short is a partial short which will not draw sufficient current to trip overcurrent protection offered by the solid state power switch.

Risk: Negligible. Low probability of occurrence, estimated at 6.3×10^{-12} .

- **84942: Launch SPF AFC Fault** - If worst-case AFC (Bus Streamer) fault occurs between Separation and AACS control (detumble), there may be up to 390 seconds before AACS begins to detumble the spacecraft.

Risk: Negligible. Fault protection response and low probability of having a combination of failures in such a short period of time.

* **Reference: Cassini Risk Assessment Review, Single Point Failure, C.P. Jones, 08/18/97**