Managing Risk to Ensure a Successful Cassini/Huygens Saturn Orbit Insertion (SOI)

Mona M. Witkowski, Shin M. Huh, John B. Burt & Julie L. Webster

Jet Propulsion Laboratory - California Institute of Technology Pasadena, CA USA

Cassini/Huygens is a planetary mission to Saturn, jointly developed by the National Aeronautics and Space Administration (NASA) and the European (ESA) and Italian Space Agencies. It was launched from the Kennedy Space Center on October 15, 1997 and is scheduled to arrive at Saturn on July 1, 2004. Upon arrival at Saturn, the Cassini/Huygens spacecraft will fire its main engine to maneuver itself into orbit around the planet. On December 25, 2004, during its third orbit, Cassini will release ESA's Huygens Probe on a trajectory bound for Titan, Saturn's largest moon. The Huygens Probe will continue on its trajectory toward Titan for the next three weeks. On January 14, 2005 it will descend through Titan's dense atmosphere and relay data and images back to the Cassini Orbiter, for transfer to Earth. Following the Huygens Probe Mission, the Cassini Orbiter will continue on to observe Saturn, its rings, many moons and icy satellites for four years of Saturn Tour Operations.

Space travel is inherently risky. Many things can go wrong and threaten the success of a mission, particularly one as complex as Cassini/Huygens. To ensure mission success, the program proactively manages risk to its spacecraft, suite of 12 instruments, Huygens Probe and operational timelines. Spacecraft redundancy, autonomy and operational timelines were specifically designed to execute the time-critical maneuver. Operational timelines are well established and Saturn Orbit Insertion (SOI) is not a resource that can be traded against others for risk reduction. SOI on July 1, 2004 is the one activity that is absolutely mission critical and essential for the success of the entire program. It is the one key event that must occur successfully, in order to allow both the Cassini Orbiter and Huygens Probe to fulfill their respective missions. The flight operations team has just one shot at SOI and failure is not an option. The success of the entire mission is dependent on a successful SOI. Managing risk to ensure a successful SOI is a high priority as the flight operations team designs, builds and tests the sequence of commands that will maneuver Cassini into orbit around Saturn.

Managing risk on Cassini/Huygens is a program level process that is coordinated by the Mission Assurance Manager and supported by the various elements of the Flight Operations Team. The flight operations team consists of many individual teams, which are distributed across both the United States and Europe. The distributed nature of the operations process represents a unique challenge to the Cassini Program, as many of the teams support risk management via telecon, email and Internet communication. The NASA/JPL Risk Management Process handles the Cassini Orbiter centric risks, including risk items pertaining to the spacecraft to probe interface. The ESA Risk Management Process handles all Huygens Probe related risk issues. While dual risk management processes are in place, the NASA/JPL process is responsible for ensuring that interface risk areas are adequately identified, documented and mitigated. Refer to Figure 1 – Cassini Risk Management Implementation.

Cassini Risk Management Implementation

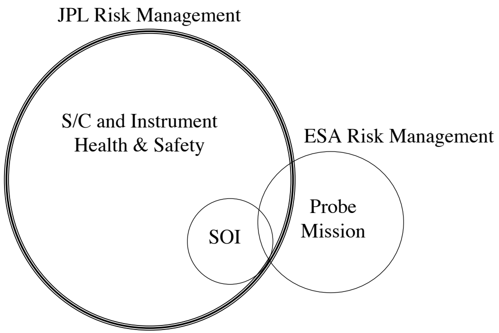

Figure 1

Risk items are captured and managed by an on-line risk management tool that is administered and controlled by the Mission Assurance Manager. This arrangement allows any user to enter risks into the system. Any team member has the authority to push the alert button and communicate a risk that causes them concern. Final disposition and mitigation efforts are discussed in an open forum, which includes all flight teams, and are approved by this risk team, prior to implementation. This open forum ensures adequate communication across team boundaries, to prevent one team from being potentially and inadvertently affected by another's mitigation efforts. This process achieves buy-in from the team as a whole, vets the risk items before the program manager and ensures that all participants are on the same page, prior to investing time and effort toward mitigation activities. Risks are evaluated, dispositioned, re-dispositioned and also eventually retired in same this manner.

Risk management is a continuous process, where-by risks are dispositioned on a quarterly basis. Risks are binned by Mission Phase, which allows the team to work on one subset of risk items at a time. Risks to SOI are managed as a subset of all risks to achieving mission success. Due to the criticality of SOI, this subset of risks is worked frequently and proactively with the spacecraft engineers who are designing and testing the sequence for this critical mission event. The Risk Management Process for Cassini SOI involves far more than the risk items captured in the online risk tool. While the online tool provides the capability to do risk management from the bottom up, other methods are necessary to completely bound the risk to SOI from a top down approach.

SOI Risk Management broadly encompasses elements of design, test, failure analysis, residual risk assessment and mission assurance. The spacecraft itself is designed to be largely single fault tolerant and has sophisticated fault protection software to detect and correct failures. All critical engineering components on Cassini are redundant. In the event of a problem or failure, fault protection will attempt to resolve it and if necessary, swap components and call safing. Flight software is designed to place the spacecraft into a "safe" state in the event that it encounters an error that it can not correct on its own. In that "safe" state, the spacecraft is safe from harm while it waits for ground intervention, to tell it what to do next. The spacecraft routine operations are conducted in a flight-demonstrated envelope, with margin. Daily flight operations must be conducted in compliance with stringent requirements and flight rules, which are checked and rechecked prior to each activity. During the SOI sequence, the spacecraft will be operated in “critical” mode, which allows certain aspects of fault protection to be disabled. This will allow non-critical fault modes to be present, while continuing on with the sequence of events without interruption from fault protection software. In addition, the SOI critical sequence is divided into regions delineated by mark points. These mark points have been placed into the sequence to allow the flight software to recover from faults and roll back to the portion of the sequence it was executing when the fault occurred. For example, should a main engine stop during the SOI burn, fault protection would stop the burn, swap to the redundant engine and resume the burn.

The test program has been crucial to reducing risk to achieving SOI. The policy of “fly as you test and test as you fly” has been critical to identifying risk areas and correcting them prior to the actual event. The sequence was first baselined and then severely fault and stress tested using both hardware and software flight system testbeds. Where errors were uncovered, modifications to the sequence or flight software were necessary to ensure seamless execution. There were occasions when the critical sequence uncovered deficiencies in the flight software that had to be fixed in order to allow the sequence to successfully run to completion. The sequence was tested and retested, following each modification to the sequence itself and/or flight software. The SOI versions of flight software were frozen in mid 2001 and were successfully uplinked to the spacecraft in early 2002. Following approximately two months of in-flight checkout activity, both the Command and Data Subsystem (CDS) and Attitude and Articulation Control Subsystem (AACS) flight software were configured as prime. They have been controlling and operating the spacecraft flawlessly now for over a year. Testing onboard the spacecraft prior to SOI has also been critical to validating spacecraft events and contingency plans. Numerous in-flight checkouts and demonstrations have been executed to remove first time events and perceived risk areas, prior to SOI.

Failure analysis has been the focus of many spacecraft engineers designing the ground activity and contingency plans. SOI is a critical event that is made up of many smaller critical events, all of which must occur successfully. With this in mind, an exhaustive effort was conducted to generate a critical event driven fault tree. Each critical event was analyzed for potential fault cases which were then traced down further, through fault trees. Each event tree terminates with ‘corrected by spacecraft autonomy’, or risk mitigation and contingency measures are required to recover. A separate analysis of the Critical Event Timeline was performed, to identify dependencies between events, as well as possible failure impacts from one event on downstream events. The ‘cross activity planning’ effort identified places where the timeline was tight and additional contingency actions which may be necessary to recover. Refer to Figure 2 – SOI Event Fault Tree.

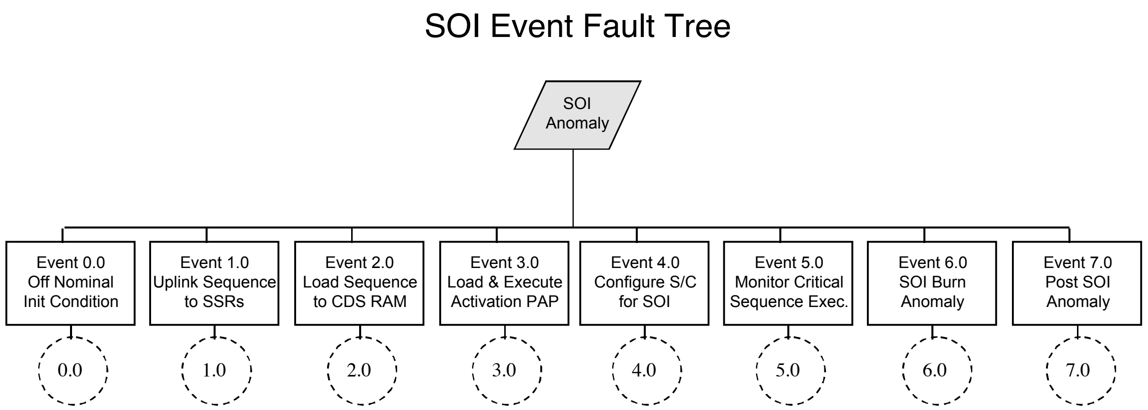
SOI Event Fault Tree
SOI Anomaly
Event 0.0 Off Nominal Init Condition
Event 1.0 Uplink Sequence to SSRs
Event 2.0 Load Sequence to CDS RAM
Event 3.0 Load & Execute Activation PAP
Event 4.0 Configure S/C for SOI
Event 5.0 Monitor Critical Sequence Exec.
Event 6.0 SOI Burn Anomaly
Event 7.0 Post SOI Anomaly
0.0
1.0
2.0
3.0
4.0
5.0
6.0
7.0

Figure 2

Contingency plans have been developed and validated during in-flight demonstrations. The entire SOI Critical Sequence (with the exception of the engine burn and pyro commands) was successfully uplinked, executed and validated onboard the spacecraft in July 2003. This in-flight demonstration was instrumental in validating both the critical sequence and the respective contingency plans. In addition, pre-launch red flag Problem Failure Reports (PFRs), waivers and single point failures were closely scrutinized again, now seven years since launch, and characterized to identify whether any residual risk areas remain. This effort did not introduce any risk item that was not already documented and mitigated appropriately. As an added measure of assurance, a Probabilistic Risk Assessment (PRA) was considered to provide an independent analysis to assist the program in prioritizing risks and validating the current approach. While it was beneficial to have a PRA analyst independently review the fault trees and contingency plans, it was determined that any PRA generated at this point in the mission would provide little value. This being due to the nature of the SOI critical event itself, the timeframe remaining until the actual event and the fact that Cassini was designed to be single-fault tolerant, regardless of the probability of the fault occurring.

Finally, Cassini has implemented a disciplined mission assurance process to appropriately characterize variances in flight, through the use of Incident Surprise Anomaly Reports (ISAs), PFRs and Waivers. All variances undergo an independent evaluation and risk assessment, performed by the Mission Assurance Manager. A full time Mission Assurance Manager is on staff and reports directly to both the Program Manager and the JPL Office of Safety and Mission Success, to independently assess compliance with institutional standards, provide on-going independent risk assessments and communicate lessons learned from other missions in flight operations. Operations errors are a significant concern for long missions, like Cassini, where new personnel rotate in often. Processes are strictly controlled and ISAs are used to help identify possible areas for improved checking or analysis in uplink or downlink processes.

In addition to the effort conducted by the Cassini Program and Flight Operations Team to proactively manage risk, independent assessments were also conducted at key phases during the SOI critical event planning process. A Preliminary Design Review was conducted in October 2000, followed by a very detailed Sequence Design/Risk Review in February 2002 and an SOI Risk Review in October 2003. Further risk reduction efforts were undertaken by developing and implementing a flight software "Smartburn" algorithm. This new algorithm design was independently risk assessed and extensively peer reviewed by attitude control experts at JPL. Several risk reviews were also conducted, targeting all areas of the SOI Critical Event, from high level communications strategies, to critical event scenarios, critical sequence design, fault protection strategies and contingency planning. As a result of these risk reviews, the communications strategy was modified to allow Cassini to communicate with Earth via the low-gain antenna during the SOI burn. This will allow the spacecraft carrier to be received during the burn, with the exception of occultations by the rings. Cassini will reconfigure back to the high gain antenna to "call home" following the burn, signaling a successful burn prior to executing post SOI science observations. Refer to Figure 3 – Communication Strategy.

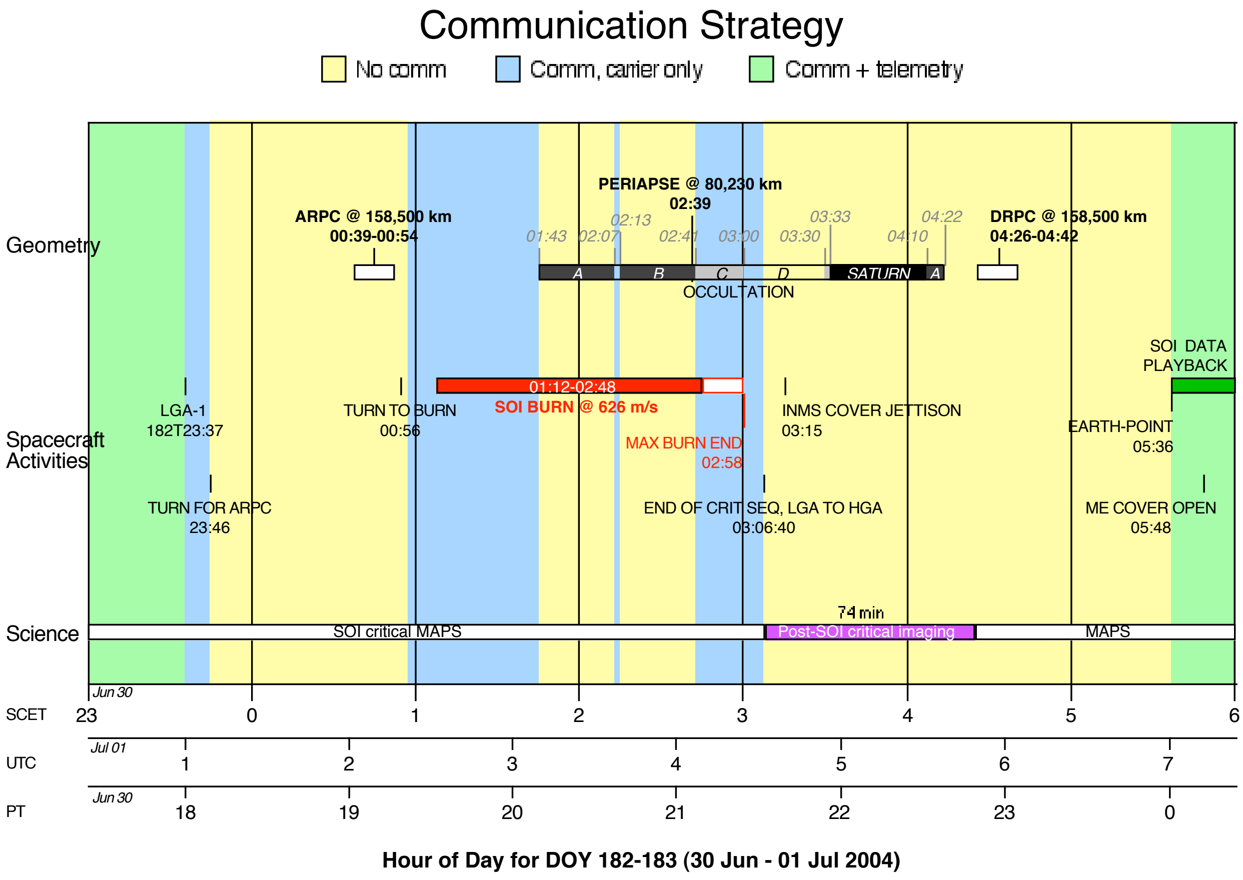

Figure 3

The Cassini/Huygens flight operations team has broadly bounded the potential risk space to achieving a successful SOI. Spacecraft engineers have worked exhaustively to develop detailed, critical event driven fault trees which bottom out at well thought out mitigation efforts and contingency plans. Some of these scenarios have been validated in-flight, others have been validated on the flight system testbed. They will continue to be validated as the team runs through its procedures in preparation for SOI. Independent assessments have been conducted to validate that the risk space has been adequately assessed and to ensure that there are no risks that haven't been identified. Finally, numerous risk reviews have been held to assess progress against plans and obtain feedback from engineering and risk management professionals. The Cassini/Huygens team has thoroughly bounded the risk space for SOI and is ready for a successful Saturn Orbit Insertion on 1 July 2004.

This paper documents the detailed, rigorous risk management process that the Cassini/Huygens program has implemented to ensure a successful SOI. It is hoped that others can learn and benefit from the approach Cassini/Huygens has taken to manage risk regarding the single most important phase of its mission – SOI. The risk management effort, described in this paper, was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration.