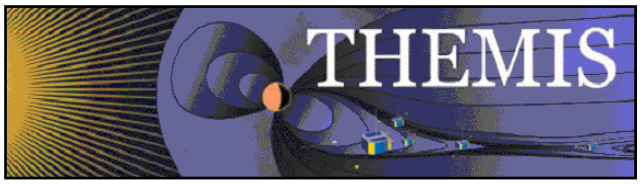


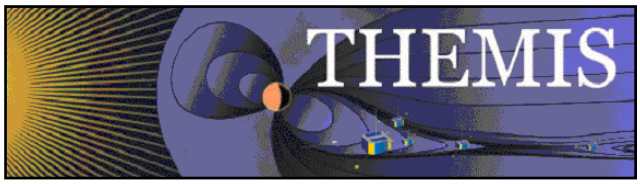
THEMIS
Fault Tree Analysis (FTA)

THM-SYS-016a
May 21, 2004

Ellen Taylor, U.C.Berkeley THEMIS Mission Systems Engineer

Kevin Brenneman, Swales Aerospace, THEMIS Spacecraft Systems Engineer

Peter Harvey, U.C.Berkeley THEMIS Project Manager



Document Revision Record

Rev.	Date	Description of Change	Approved By
-	11/12/03	FTA completed in Phase A CSR and presented at PDR	-
A	05/21/04	FTA Document developed to clearly state objectives, assumptions and conclusions	ERT

Distribution List

Name	Email
Vassilis Angelopoulos, PI, U.C. Berkeley	vassilis@ssl.berkeley.edu;
Peter Harvey, Project Manager, U.C.Berkeley	prh@ssl.berkeley.edu;
Ellen Taylor, Mission Systems, U.C. Berkeley	ertaylor@ssl.berkeley.edu;
Tom Ajluni, System Engineer, Swales Aerospace	tajluni@swales.com;
Kevin Brenneman, Probe Systems, Swales Aerospace	kbrenneman@swales.com;
Mike Cully, Probe Project Manager, Swales Aerospace	mcully@swales.com;
Adrian Rad, Probe Reliability Engineer, Swales Aerospace	arad@swales.com

TBD List

Identifier	Description

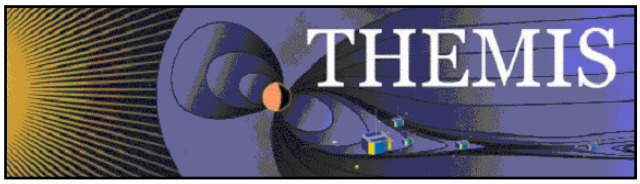
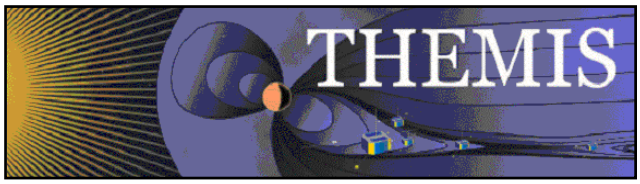


Table of Contents



1. OVERVIEW

THEMIS is a NASA Explorer mission which will launch a constellation of five micro-satellites (probes) in mid-2006. Flying in synchronous orbits within the earth's magnetosphere, the probes will measure the particle processes responsible for eruptions of the aurora.

The THEMIS Fault Tree Analysis (FTA) is developed to clearly depict potential faults during all mission phases as related to minimum and baseline success criteria. The FTA is then used as a basis for evaluating the severity of faults in the Probabilistic Risk Assessment (PRA) and Failure Modes and Effects Analysis (FMEA). In this context, the FTA focuses on two principle components to the THEMIS mission:

(1) Constellation redundancy and the use of an on-orbit spare. P3 or P4 probes can replace any other probe during the first year of the mission, resulting in a 4- probe configuration that can accomplish the minimum performance science within 1 year, and near baseline science goals of the mission within 2 years; and

(2) Science resilience. Minimum science can still be accomplished with partial or total sensor failure on one or more of the probes.

1.1 SCOPE

The THEMIS approach to Reliability Engineering is provided in *THM-SYS-006 Systems Engineering Management Plan (SEMP)*. The SEMP identifies the type of reliability analyses that will be performed for mission, and the modeling tools and techniques that will be used. To summarize, a Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA) and Probabilistic Risk Assessment (PRA) are completed during the preliminary and detailed design phases to evaluate the robustness of the system design and the reliability of the overall mission. An Event Tree Analysis (ETA) is then completed in Phase C/D as a tool for operations and contingency planning.

The FTA, as described here, was prepared in Phase A and continues to be valid due to very little change in the overall system architecture. Beginning with an undesired state (mission failure or degraded mission), the fault tree includes all credible combinations of events/faults that could lead to that state. The fault tree in itself is not a quantitative model, but becomes a quantitative assessment when combined with the PRA, as described in *THM-SYS-017 THEMIS Probabilistic Risk Assessment (PRA)*.

1.2 PURPOSE

The purpose of this FTA is to provide an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed to find all credible ways in which the undesired event can occur. The FTA provides a methodical approach to understanding the system and its operation. Through this understanding, informed decisions guiding the mission design and system architecture can be made.

1.3 OBJECTIVES

The main objectives of this FTA are to:

- Address both mission failures and degraded modes of operation in accordance with the mission requirements and minimum/baseline success criteria;
- Evaluate the result of element "block" failure, regardless of cause to identify the level of fault tolerance in the system (single-point failures, 1 fault tolerance, 2 fault tolerance, >2 fault tolerances); and

- Provide a means for assessing (along with the PRA and FMEA) the overall reliability of the system.

2. SUCCESS CRITERIA

To thoroughly evaluate the Fault Tolerance of a system, there must be a clear understanding of the how failures affect minimum and baseline science objectives during each mission phase. Minimum and Baseline success criteria are provided in *THEMIS Level 1 Science Requirements*. Below is a discussion of how specific failures during each mission phase affects the Level 1 Requirements. The discussion is taken in part from the THEMIS Replacement Strategy (*System Requirement Review RFA #15*) as the same logic will be used to determine if a Probe must be replaced on-orbit.

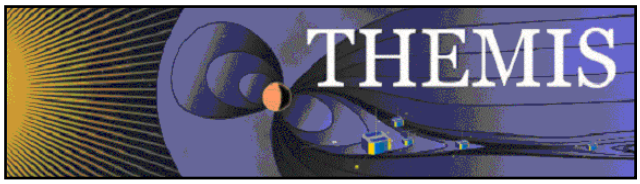
2.1 DEFINITION OF A FAILED PROBE

In accordance with the minimum mission requirement to monitor with two probes each the current disruption (P3, P4) and reconnection (P1 and P2) process, the minimum mission can be accomplished by P1-P4. However not all instruments are needed to perform minimum mission measurements. Figure 1 shows in red the instruments required to perform minimum mission measurements.

Instruments required to achieve Primary Mission Objective						
	Measurement goals	P1	P2	P3	P4	P5
Time History of Events	P3,4&5 monitor CD P1,2 bracket Rx t_{res}<30s, $\delta Y<\pm 2R_E$	FGM 2SSTh 2EFIs	FGM ESA 2SSTh 2EFIs	FGM ESA 1SSTh	FGM ESA 1SSTh	FGM ESA 1SSTh
Macroscale Interactions	Track rarefaction wave, inward flows, Poynting with $\delta B<1nT$, $\delta V/V\sim 10\%$		FGM ESA	FGM ESA	FGM ESA	FGM ESA
	Radial/cross-sheet pressure, velocity and current gradients require $\delta P/P\sim \delta V/V \sim \delta B/B \sim 10\%$, non-MHD		FGM ESA	FGM ESA 2EFIs	FGM ESA 2EFIs	FGM ESA 2EFIs
	Cross-tail pairs measure FLRs, KH, ballooning on B, V, P @ 10s and fast modes on B_{xyz} and E_{xy} @ 6Hz		FGM ESA	FGM ESA	FGM ESA	FGM ESA

Figure 1: Instruments required for Minimum Mission

The decision on instrument partial versus complete failure will be made after appropriate diagnostics tests and in consultation with the cognizant mechanical engineer, lead scientist and science team. The question to be answered is whether the minimum science objectives are violated by the condition or anomaly at hand, whether technical or scientific workarounds are possible at an instrument level or at a mission level.



2.2 REPLACEMENT STRATEGY PRIOR TO 1st YEAR TAIL SEASON

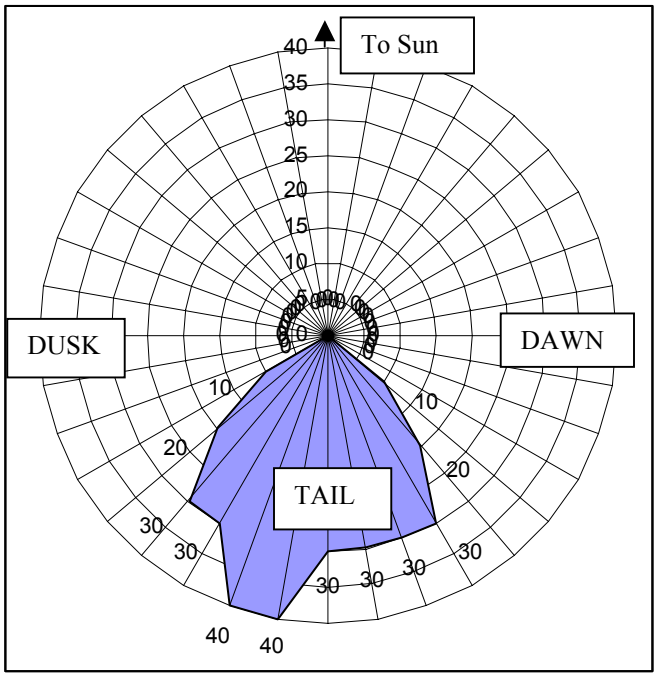
Contingency replacement is the process by which a probe that is critical to the accomplishment of the minimum mission goals is replaced by another probe, in order to achieve minimum mission objectives. Since the minimum mission requirements are met by the current baseline orbit design within the first year of operations, contingency replacement is exercised only if a mission-critical probe becomes inoperable (i.e., unable to fulfill its role to achieve minimum mission) at or prior to the first-year tail season.

Should minimum mission objectives be partially satisfied due to the time of the failure (e.g., mid-way through 1st tail season) then probe replacement and the time/process for replacement are evaluated in light of the effects of that replacement on second-year mission quality. The general guidelines for P1/P2 replacement by any of P3/P4/P5 are shown below in Table 1, as function of the time when the decision to replace has been taken.

The following points clarify how this table was constructed. LD stands for Launch Day, nominally October 21, 2006. WD stands for Wedding Day, February 23, 2007.

- Since probes are assigned their positions at LD+16d, no replacement is envisioned earlier in the mission.
- Worst case scenario are studied: e.g., probe fails at the worst time in the interval considered, and takes the longest agreed-upon time for the failure to be acknowledged, resolved or replacement decision to be taken.
- "Failed" probe in bold denotes the probe number that failed. The explanations in the same cell after it remind us what position the failed probe was in, and what condition other relevant probes where in.
- Date to start replacement denotes the date by which all actions on instrument recovery or probe resuscitation have been closed, and a decision to replace the probe has already been taken; the date denotes the closest day to the start of the replacement in accordance with the replacement operational plan already completed while instrument diagnostics were being made.
- Replacement strategy explains which probe replaces which in the constellation.
- Maneuver strategy explains how the replacement is to be made. Main question is if radial wires are out or not. If they are it is very inefficient (fuel-wise) to replace by reor-fire-reor sequence. It is more efficient to replace by side-thrusting.
- Replacement duration is a rough estimate to perform the complete replacement of the failed probe.
- Minimum science before failure is the percentage of minimum science (94hrs, see L1 requirements) into the 1st tail season prior to the probe's failure, that the constellation was in position performing nominal science observations. This results in accumulation of useful substorm events towards meeting minimum science goals and plays into the evaluation of whether minimum science is met and thus whether replacement is warranted. Note that not all conjunctions are equal. The highest quality conjunctions, i.e., those that have higher probability to lead to substorm observations, are those closest to the midnight sector, with a slight bias towards dusk (i.e., after WD). This factor is roughly evaluated in the computation of minimum science before failure.

- Assuming that the constellation was in place during the period prior to the failure, a sudden death of the failed probe results in full accumulation prior to failure, but a slow deterioration of the instrument/probe health, or an (unforeseen) late detection of a data quality loss, results in partial data recovery and eats into the useful conjunctions which count towards minimum science. This means that the MOC and SOC teams much be vigilant about early detection of anomalies and ensuring that science evaluation is performed shortly after data acquisition.
- Minimum science after replacement is the percentage of minimum science (94hrs, see L1 requirements) of the 1st tail season after the failed probe's replacement, that the constellation was in position performing minimum science observations. This results in accumulation of useful substorm events towards meeting minimum science goals and plays into the evaluation of whether minimum science is met by the mission during the first year and thus whether replacement during the first year is warranted. Note that not all conjunctions are equal. The highest quality conjunctions, i.e., those that have higher probability to lead to substorm observations, are those closest to the midnight sector, with a slight bias towards dusk (i.e., after WD). This is factored in the computation of minimum science after replacement.
- Minimum mission accomplished? When? This simply states if the minimum science is accomplished in the 1st year and by which time in the 1st year tail season. It is strictly based on the summation of the minimum science before failure and after replacement.
- Rough estimate of % of minimum science yield within a 10day interval as function of season is shown below (10-day divisions are shown). The angle represents the time of the year; Sunward is at the top; Dawn to the right, etc. The anticipated percentage of minimum science yield (94hrs) is shown by the chart to range from 10%/10days closer to dawn and dusk (i.e., near WD+60d and WD+60d) to 40%/10days closer to midnight, with preference near the post-midnight sector.



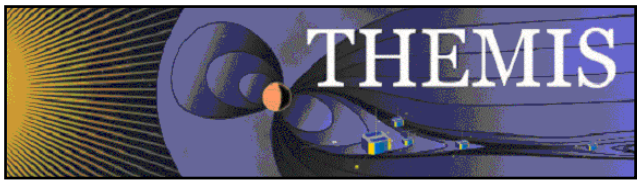


Table 1. Replacement strategy of probe P1/P2 by probes P3 or P4, depending on the time of failure.							
"**Failed**" probe, under what condition	Date to start replacement (calculations assume latest one)	**Replacement probe**, strategy	Maneuver strategy	Replacement duration	Minimum science before failure	Minimum science 1st year after replacement	Minimum mission accomplished? When?
P1 replacement							
P1 ascending, P5 wires in	[LD+16, WD-90)	**P5**->P1	Reor-fire-reor	<10days	0%	300%	YES, within 1st tail season
P1 in place, P5 wires in	[WD-90, WD-60)	**P5**->P1	Reor-fire-reor	<10days	0%	290%	YES, within 1st tail season
P1 in place, P5 wires out	[WD-60, WD-30)	**P3**->P1 P5->P3	Side-thrusting	20days	30% (sudden death)	200%	YES, within 1st tail season
P1 in place, P5 wires out	[WD-60, WD-30)	**P3**->P1 P5->P3	Side-thrusting	20days	0% (sick, detected late)	200%	YES, within 1st tail season
P1 in place, P5 wires out	[WD-30, WD)	**P3**->P1 P5->P3	Side-thrusting	20days	120% (sudden death)	90%	YES, within 1st tail season
P1 in place, P5 wires out	[WD-30, WD)	**P3**->P1 P5->P3	Side-thrusting	20days	60% (sick, detected late)	90%	YES, within 1st tail season
P1 in place, P5 wires out	[WD, WD+30)	~~**P3**->P1 P5->P3~~	Side-thrusting	20days	190% (sudden death)	10%	YES, within 1st tail season
P1 in place, P5 wires out	[WD, WD+30)	~~**P3**->P1 P5->P3~~	Side-thrusting	20days	120% (sick, detected late)	10%	YES, within 1st tail season
P1 in place, P5 wires out	[WD+30, WD+60)	~~**P3**->P1 P5->P3~~	Side-thrusting	20days	290% (sudden death)	0%	YES, within 1st tail season
P1 in place, P5 wires out	[WD+30, WD+60)	~~**P3**->P1 P5->P3~~	Side-thrusting	20days	240% (sick, detected late)	0%	YES, within 1st tail season
P2 replacement							
P2 ascending, P5 wires in	[LD+16, WD-90)	**P5**->P2	Reor-fire-reor	<5days	0%	300%	YES, within 1st tail season
P2 in place, P5 wires in	[WD-90, WD-60)	**P5**->P2	Reor-fire-reor	<5days	0%	295%	YES, within 1st tail season
P2 in place, P5 wires out	[WD-60, WD-30)	**P3**->P2 P5->P3	Side-thrusting	10days	30% (sudden death)	230%	YES, within 1st tail season
P2 in place, P5 wires out	[WD-60, WD-30)	**P3**->P2 P5->P3	Side-thrusting	10days	0% (sick, detected late)	230%	YES, within 1st tail season
P2 in place, P5 wires out	[WD-30, WD)	**P3**->P2 P5->P3	Side-thrusting	10days	120% (sudden death)	130%	YES, within 1st tail season
P2 in place, P5 wires out	[WD-30, WD)	**P3**->P2 P5->P3	Side-thrusting	10days	60% (sick, detected late)	130%	YES, within 1st tail season
P2 in place, P5 wires out	[WD, WD+30)	~~**P3**->P2 P5->P3~~	Side-thrusting	10days	190% (sudden death)	30%	YES, within 1st tail season
P2 in place, P5 wires out	[WD, WD+30)	~~**P3**->P2 P5->P3~~	Side-thrusting	10days	120% (sick, detected late)	30%	YES, within 1st tail season
P2 in place, P5 wires out	[WD+30, WD+60)	~~**P3**->P2 P5->P3~~	Side-thrusting	10days	290% (sudden death)	0%	YES, within 1st tail season
P2 in place, P5 wires out	[WD+30, WD+60)	~~**P3**->P2 P5->P3~~	Side-thrusting	10days	240% (sick, detected late)	0%	YES, within 1st tail season

2.3 REPLACEMENT STRATEGY AFTER 1st YEAR TAIL SEASON

From Table 1, the replacement of P1/P2 in order to achieve the minimum science is necessary if a probe fails prior to WD-30 and helpful if a probe fails between WD-30 and WD. However replacement of a probe is not necessary to meet minimum science if a probe fails after WD. In that case, other considerations will play a role in the replacement decision, which is scheduled to happen 9 months later, in preparation of the 2nd year tail season.

If the replacement is to start at WD or thereafter, the benefits to the minimum science are very small (10-30% of minimum science), while under worst conditions (degrading probe detected 20days late) the minimum science is still recovered from conjunctions prior to the failure (120%, for P1 failure within prime – postmidnight-- science location detected as late as WD+20d). Therefore the following options have been considered:

1. Replace the failed probe in anticipation of second year science. This replacement can take place immediately or be delayed for 3 months (in anticipation of dayside science) or 6 months (in anticipation of second year tail science). Replacement retrieves dayside science, but does not retrieve baseline science which necessitate 3 inner probes.
   - Replace immediately: The differential precession in Right Ascension of Perigee between P1 and P3/5 will grow without obvious effects to the second year tail science.
   - Replace after 3 months: There is sufficient time to analyze tail science data, and ensure that additional four-probe data are necessary from 2nd yr to address minimum science. Dayside science can still be obtained with minor degradation as planned.
   - Replace after 9 months: There is plenty of time to analyze 1st year tail science data and make a well informed decision as to the quality and importance of conjunctions obtained; and whether additional data are needed. 1st year dayside science cannot be obtained. 2nd year dayside science is still possible.
2. Assuming the substorm problem has been solved from 1st year tail science already, and assuming sufficient fuel reserves remain, then position probes to perform the additional baseline science during the 2nd year of operations:
   - If P1 is the failed probe, then P3/4/5 continue to go through their nominal 2nd yr maneuvers.
   - If P2 is the failed probe, and sufficient reserves remain in P1, then lower P1 apogee to P2's prior to 2nd year tail season.

After considering these options available in the case of P1 failure after WD, it is deemed most reasonable to delay the P1 ascend for 9 months; this option permits recovery of baseline tail science and 2nd year dayside science, i.e., results in maximum recovery of THEMIS's baseline science objectives. Should P2 were to fail, then P1 fuel reserves would be evaluated to determine if its apogee can be reduced to P2's and action would be taken to perform this maneuver shortly thereafter. Neither plans are important for retrieval of minimum science objectives since those have already been achieved. This is the reason the respective cells have been cross-hatched in Table 1.

3. THEMIS FAULT TREE DIAGRAM

The THEMIS fault tree diagram was developed by initially assuming an undesired state as described below:

1. Loss of Mission (Below Minimum: < 4 probes or < 1 year)
2. Minimum Science Mission (At Minimum: 4 probes for 1 year)
3. Reduced Science Mission (Above Minimum: 4 probes for 2 years)
4. Near-full Science Performance (Near Baseline: 5 probes for 1 year)
5. Full Science Performance (Baseline: 5 probes for 2 years)

The system was then analyzed using the criteria set out in Section 2 above to find all credible ways the undesired event could occur. Recovery notes were added if the failure required a recovery action to maintain the state. For example, Minimum Science can be maintained of the Instrument Data Processor Unit (IDPU) on one Probe fails completely. However, the Recovery Scheme to maneuver either P3 or P4 into the replacement orbit of the failed probe must be accomplished.

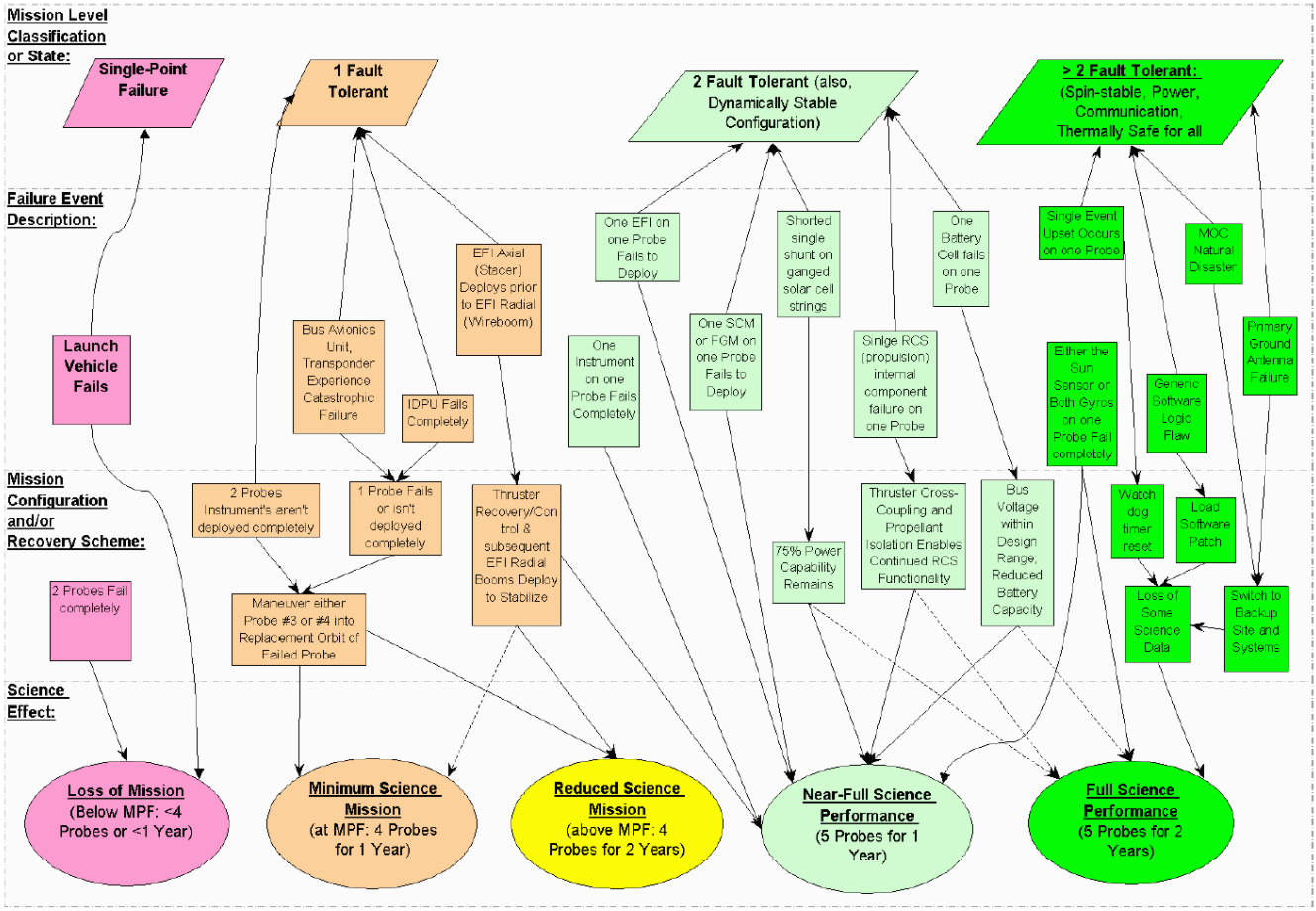
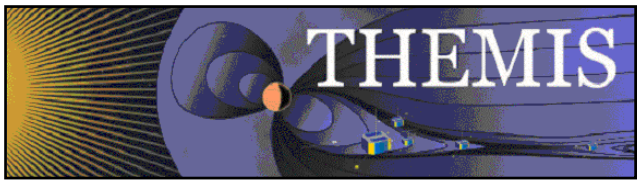


Figure 2: THEMIS Fault Tree Diagram



4. CONCLUSION

The FTA provides a roadmap for further reliability analyses. By directly relating faults to the Level 1 Science Requirements Minimum and Baseline Success Criteria, it provides a top down evaluation of which instruments (noted as red in Figure 1) and subsystems (noted as orange block failures in Figure 2) are critical to the minimum and baseline mission. Those instruments and subsystems identified deserve more scrutiny and evaluation than others. Critical events, such as boom deploy, also deserve additional attention. Specifically, these systems must be evaluated for single-point failures (in the FMEA) and reliability (in the PRA). In addition, it is evident from this FTA that the THEMIS replacement strategy must be preserved to guarantee minimum science objectives are met and the Probe single string design remains viable.