THEMIS
Failure Modes Effects and Criticality Analysis
(FMECA)

THM-SYS-007b
May 26, 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
-	10/30/03	Released Draft (Preliminary FMECA)	-
A	5/14/04	Updated Information (Final FMECA)	ERT
B	5/26/04	Added Reliability Block Diagram as Appendix D	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;
Paul Turin, Mechanical Systems Engineer, U.C. Berkeley	pturin@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. As the prime contractor for THEMIS, the University of California at Berkeley will provide the project management, systems engineering, flight instrumentation, ground-based imagers, mission operations, and performance assurance. Swales Aerospace will provide probe buses, probe bus carrier and integration and test. Key international partners include instrument teams from Canada, France, Germany, and Austria.

There are two principle components to the THEMIS mission that must be considered when completing the Mission-Level Failure Mode Effects and Criticality Analysis (FMECA) and assessing the possible single point failure modes of the 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.

Therefore, the flight system itself is predominantly single-string designs with some areas of functional redundancy. Nonetheless, this FMECA is performed both at the system and subsystem interface level to determine the basis for system robustness to potential failure modes, the data points required to detect them, and the steps that should be taken to mitigate them. Mitigation can be additional test points, redundant data paths, filtering of auxiliary telemetry data, formation of backup procedures, and additional ground software and procedures to provide failure detection and response.

1.1 SCOPE

The Mission-Level FMECA is performed early in the detailed design process to ensure appropriate redundancy in the system design and sufficient reliability of critical parts and assemblies. As the design matures, more detailed Subsystem FMECAs are completed to further identify the possible failure modes and to assess the reliability of each subsystem. These FMECAs, part the acceptance data package for each probe subsystem, are considered separate deliverables and are not contained within the scope of this document. Nevertheless, all subsystem FMECAs are evaluated as they pertain to the assumptions described here-in.

1.2 PURPOSE

The explicit purpose of this FMECA is to identify critical items in the system by assessing the impact of failure at each interface. This document also identifies a failure remedy (recommended action or response plan) to reduce the probability and/or effect of the failure. Ultimately, the FMECA will be used to create a viable test and analysis plan that focuses resources to increase reliability.

1.3 OBJECTIVES

The main objectives of the Mission-Level FMECA are to:

- Verify that redundant paths are isolated or protected such that any single failure that causes the loss of a functional path shall not affect the other functional path or the capability to switch operation to that redundant path;
- Verify that the THEMIS system has no single or redundant interface failure mode, which could affect safety of personnel, or cause catastrophic failure of the launch vehicle;
- Verify that any single point failures have sufficient reliability so as to not compromise the probability of mission success;
- Identify existing methods of failure detection and any possible need for new methods; and
- Identify any failure modes, which may be time critical for corrective action.

1.4 DEFINITIONS

- Subsystem: A combination of self-contained components.
- Component: An entire electronics chassis - a combination of parts, devices, and structures, which perform a distinct function in the operation of the overall equipment.
- Assembly: The highest order sub-division of a component. It may be a combination of circuit board module (box) or a sensor module.
- Module: An individual circuit board or distinct functional element.
- Circuit Element: A subset of an Assembly, the circuit element is a single electrical circuit, which performs a very specific function, with specified inputs and outputs. A circuit element can be analyzed stand-alone for failure modes and can be subjected to stand-alone Worst Case Analysis or Test.
- Failure: The inability of a system, subsystem, component, or assembly to perform its required function within specified limits, under specified conditions, for a specified duration.
- Failure Mode: A description of the manner in which a failure may occur.
- Corrective Action: Actions, which could be taken to circumvent the failure of an item.
- Failure Cause: Any creditable event that can generate a failure of an item or items.
- Redundancy: Multiple ways of performing a function.
- Operational Redundancy: Redundant items, all of which are fully energized during the subsystem operating cycle. Operations redundancy includes load-sharing redundancy, where redundant items are connected in such a manner that upon failure of one unit, the remaining items will continue to perform the system function.
- Standby Redundancy: Redundant hardware items that is non-operative (have no power applied) until they are switched to the subsystem upon failure of the primary item.
- Like Redundancy: Identical hardware items performing the same function.
- Unlike Redundancy: Non-identical hardware items performing the same function.

- Single Point Failure: The failure of an item which would result in permanent failure of a subsystem (i.e. degraded capability or loss of THEMIS mission), and which is not compensated for by redundancy or alternative operation procedure.

2. FMECA METHODOLOGIES AND APPLICATION

THEMIS failure analysis is conducted for all interfaces down to the subsystem level using block diagrams traceable to FMECA worksheets. Appendix A contains the Instrument Suite block diagrams. Appendix B contains the completed worksheets for the Instrument Suite. Appendix C contains the Probe Subsystem FMECA outline and reliability calculations. As mentioned above, detailed subsystem FMECAs are completed for each Probe Subsystem, but not considered within the scope of this document.

The analysis is performed by first assuming specific failure modes at a given interface or subsystem block. The effect of the failure on the subsystem function is recorded on the worksheet. Further analysis is completed to identify what circuit elements could cause the failure and what corrective actions should be taken to eliminate the failure mode. Items are identified for those circuit elements deemed mission critical. The THEMIS critical items list is provided in Section 3.2 of this document.

For the Instrument Suite FMECA, the analysis is performed for the following functional interfaces evaluated for each Instrument (ESA, SST, FGM, SCM and EFI):

1. Power Interfaces
2. Data Interfaces

For the Probe Bus Suite FMECA, the analysis is performed for the following subsystem functional blocks:

1. Electrical Power Subsystem
2. Attitude Control Subsystem
3. Reaction Control Subsystem
4. Communication Subsystem
3. C&DH/Processor Subsystem
4. Backplane
5. Harness/Grounding
6. Separation Subsystem

2.1 ASSUMPTIONS

This FMECA was performed under the following assumptions:

- It is assumed that only one failure mode has occurred at any given time, thus establishing the critically category for the failure modes.
- It is assumed that identical boards in different probes do not have a common design flaw that would cause something other than an uncorrelated or random failure.
- Failures that may occur during ground operations are not addressed.
- The power distribution interface failures considered were (1) loss of power; (2) incorrect supply voltage (specifically under-voltage); or (3) over-current
- The data interface failures considered were (1) loss of sensor signal; (2) intermittent data from the sensor; or (3) corrupted sensor data

- The mechanism failures were considered in the context of electrical failure to initiate activation. Mechanical failures (analysis to show actuation torques and forces are at least 3 times the combined worst case resistance torques or forces predicted) have been assessed for each mechanism, but are not considered within the scope of this FMECA.
- Various failure modes specific to each Probe Subsystem were considered

2.2 WORKSHEET DEFINITIONS

For the Instrument Suite, separate FMECA worksheets were developed for each functional interface (power and data). Worksheets are provided in Appendix B. The worksheet format and quantification scales were adapted from the *JPL FMEA Worksheet* originated by A. Dembski. In conjunction with the block diagrams, the worksheet explicitly identifies potential failure modes for each interface and provides an assessment of the failure's impact on overall system reliability. Potential failures are analyzed for their likelihood and detect-ability to establish a Failure Priority Number (FPN). The highest FPN value items require the most attention. The worksheet also provides direct trace-ability for each item by capturing action plans and current status of the high FPN items.

Worksheet attributes are provided in the table below:

COLUMN HEADER	**DEFINITION**
FMECA Item Code	Unique number assigned to the functional interface under analysis.
Interface	Concise statement of the functional interface.
Potential Failure Modes	Concise statement of each failure mode possible at the designated interface.
Potential Failure Effects	Effects of the failure mode on module, component, subsystem, system, or LV.
Severity (Sev)	On a scale of 1-10, the severity of each failure (10=most severe). See severity table below.
Potential Cause	Concise statement of the potential cause(s) of the interface failure.
Probability (Prob)	On a scale of 1-10, the probability of the failure occurring. See probability table below.
Current Design Controls	Examination of the current design as applied to the failure mode. Specifically includes: the detection method for each failure mode; action, automatic or manual, that may be taken in the event of the failure; description of alternate means of operation; and/or redundancy available after a failure. Current design controls are considered heavily when considering the recommended action.
Detect-ability (Det)	On a scale of 1-10, the ability to detect if the failure occurred. See detect-ability table below.
Risk Priority Number	The combined weighting of severity, likelihood, and detect-ability. FPN=(Sev x Prob x Det)/3.
Recommended Action	Concise statement of response plan as required.
Responsibility and Target Completion Date	Identification of person responsible to implement response plan by a specific milestone.
Action Taken	Concise statement of action that was taken.
New Sev, Prob, Det, FPN	Re-evaluation of failure mode.

Definitions probability of occurrence and ability to detect are provided in the tables below.

DETECT-ABILITY	Likelihood of detection by Design Control	Ranking
Absolute Uncertainty	Design control cannot detect potential cause and subsequent failure mode	10
Very Remote	Very remote chance the design control will detect potential cause and subsequent failure mode	9
Remote	Remote chance the design control will detect potential cause and subsequent failure mode	8
Very Low	Very low chance the design control will detect potential cause and subsequent failure mode	7
Low	Low chance the design control will detect potential cause and subsequent failure mode	6
Moderate	Moderate chance the design control will detect potential cause and subsequent failure mode	5
Moderately High	Moderately High chance the design control will detect potential cause and subsequent failure mode	4
High	High chance the design control will detect potential cause and subsequent failure mode	3
Very High	Very high chance the design control will detect potential cause and subsequent failure mode	2
Almost Certain	Design control will detect potential cause and subsequent failure mode	1

PROBALITY	Ranking
Very High: Failure is almost inevitable	10
High-Very High	9
High: Repeated failures	8
Moderate-High	7
Moderate: Occasional failures	6
Moderate-Low	5
Low-Moderate	4
Low: Relatively few failures	3
Remote-Low	2
Remote: Failure is unlikely	1

3. FMECA RESULTS

For the Instrument Suite, a Failure Priority Number (FPN) was assigned to each interface. The FPN was then used identify the Failure Severity. For the Probe Bus, reliability calculations were completed for each subsystem as provided in the Appendix C spreadsheet. The Failure Severity was assessed individually for each possible failure mechanism within a probe subsystem. Although the method of identifying the severity of failures was different for the Instrument and Probe Systems, the consequences were evaluated collectively to provide a comprehensive assessment of the full system. The Failure Severity (consequence) categories are provided below:

- Level 5: Death/Injury or One or More Personnel; Loss/Damage to Launch Vehicle
- Level 4: Complete Loss of More than One Probe (loss of minimum mission)

- Level 3: Major Compromise of Probe Mission Usefulness (Retention of minimum mission but major degradation of mission performance)
- Level 2: Some Compromise of Probe Mission Usefulness (Minor loss of some mission performance)
- Level 1: No effect upon Probe Mission Usefulness

Because of the inherent constellation redundancy on THEMIS, it is assumed that a loss of the THEMIS Mission requires the loss of more than one Probe. Degradation consists the loss of one Probe or degraded performance in more than one Probe.

3.1 IDENTIFICATION OF PROBLEM AREAS

3.1.1 Level 5 Failures

No Level 5 failure modes were identified for the THEMIS System. Three subsystems were identified that could potentially cause death or injury and/or have a catastrophic effect on the launch vehicle:

1. Separation system - inadvertent separation of a probe or probes during ascent.
2. Boom Deploy - inadvertent release of the Magnetometer Booms or the Axial EFI Booms.
3. RCS Subsystem - failure of Pressurant system valve

However, as dictated by safety, all systems require three separate inhibitors. Therefore, no single failure of any of these inhibitors could have a catastrophic effect. Those interfaces with a FPN above 180 or Hazardous were considered Level 1: Catastrophic (RED).

3.1.2 Level 4 Failures

Level 4 failures included loss of one Probe, or significant (de-habilitating) problems. They also have a fairly high probability of occurrence and/or minimal ability to detect the failure. These failures include loss of core THEMIS functions on one Probe (power distribution, data collection, etc.) Those interfaces with a FPN of 40-200 are considered Level 2: Critical (YELLOW).

3.1.3 Level 3 Failures

Level 3 failures included significant degradation of the THEMIS Mission. They also have some probability of occurrence and/or uncertain ability to detect the failure. These failures included timing, experiment quality and thermal considerations. Those interfaces with a FPN of 20-40 were considered Level 3: Significant (YELLOW).

3.1.4 Level 2 Failures

Level 2 failures included minor degradation of the THEMIS Mission. They also have a low probability of occurrence and/or ability to detect the failure. These failures included slightly compromised data. Those interfaces with a FPN of 10-20 were considered Level 2: Minor (GREEN).

3.1.5 Level 1 Failures

Level 1 failures have no effect on the THEMIS Mission. Those interfaces with a FPN of 0-10 were considered Level 1: Insignificant (GREEN).

3.2 CRITICAL ITEMS LIST

From the FMECA worksheets, Level 2, 3, and 4 Failures are easily identified. The following subsystem or circuit elements were shown to be a significant aspect of the potential cause or mechanism for Level 3 and 4 failures. Mitigation techniques for these critical items are provided in the subsequent section.

1. Separation Subsystem
2. Receiver
3. Transponder
4. Bus Avionics Unit Coldfire Processor Board
5. Instrument Data Processor 8085 CPU
6. Instrument and Probe Bus FPGAs
7. Instrument and Probe Bus FETs

Separate Subsystem FMECAs will be completed for the critical Probe Subsystems (Separation Subsystem, Receiver, Transponder, BAU Processor Board) and will be available prior to the Probe Bus Pre-Environmental Review (PER).

3.3 FAILURE PREVENTION AND MITIGATION TECHNIQUES

3.3.1 Circuit Selection

Circuit elements are studied from the critical items list and, on a case-by-case basis, the best method for adding redundancy or ensuring reliability is recommended (*See Worksheet*). Additional *analyses (See Section 3.3.2)* are identified to ensure that parts are properly derated, lifetime issues are considered, and failure modes are identifiable or have compensating measures. Additional *tests (See Section 3.3.3)* are identified to ensure that circuit elements have adequate design margin, interact properly as a system, and do not have excessive sensitivity. Recommended analyses and tests are described in the following sections.

3.3.2 Analysis Techniques

Four types of analyses/simulations are recommended to ensure reliability: Parts Stress; Worst Case; Thermal; and Timing/Frequency simulations. The purpose and methodology is described below.

3.3.2.1 Parts Stress Analysis (PSA)

PSA examines all of the components in a circuit to ensure parts operate within their prescribed guidelines under all input conditions (change in Power Supply voltage, change in temperature, change in load, etc.). Standard derating criteria has been established for THEMIS parts per the Performance Assurance and Implementation Plan (PAIP). However, PSA provides additional insight into details that could cause premature circuit failure, ensuring that there are no fundamental design flaws that would affect the lifetime of components within a circuit. PSA does not analyze the performance of the circuit. It simply looks to see if any part of the circuit under a stress situation would cause premature failure.

3.3.2.2 Worst-Case Analysis (WCA)

WCA looks at lifetime and performance issues and is appropriate for circuits whose performance degradation cannot be reasonably compensated for. WCA is secondary to PSA. PSA must be performed first. In deciding which circuits required WCA, their function was considered within the context of the whole Subsystem as well as their failure consequences within the context of the FMECA.

3.3.2.3 Thermal Analysis

Performed at the board level, thermal analysis uses: expected parts placement on a circuit board; power consumption; conductivity between part leads and part junction; conductivity of circuit board and housing; and reference plate temperature to derive predicted junction temperatures and at the extreme operational conditions for all components. The PSA and thermal analysis must be consistent in that the PSA's assumed temperatures must agree with those worst-case operational junction temperatures predicted by the model.

3.3.2.4 Timing and Frequency Simulations

Timing and Frequency simulations are capable of simulating FPGA performance under given set of test vectors to ensure adequate timing margin, etc. exists in the design. These tests are particularly important in the case of the Actel FPGA's because non-flight units used for testing may have a slight speed advantage over flight chips. That is, timing margin could be adequate for the prototypes and marginal or inadequate for the flight units.

3.3.3 Test Techniques

Recommended tests ensure necessary design margin against external parameters such as operational voltage, temperature, etc. or against frequency of operation (timing margin) and input noise. Two such tests performed at either the circuit or circuit board (subsystem) level are Voltage/Temperature Margin and Frequency.

3.3.3.1 Voltage Margin Testing

Voltage Margin Testing requires varying the operational voltage (provided by an external supply) and the operational temperature to values outside those specified. By evaluating the performance of a circuit under these conditions, information similar to that attained with WCA can be obtained. This test is particularly useful for complex circuits that interact in ways that are difficult to simulate analytically. It is also useful for digital circuits such as FPGA's which don't lend themselves easily to WCA and is a useful augmentation to the time/frequency margin analysis and test. Voltage Margin Testing is recommended for a number of circuits as the most appropriate way to test the robustness of the design and to attain insight on long-term performance.

3.3.3.2 Frequency Margin Testing

Although it is useful to perform analytical simulations with predetermined test vectors and variable clock rates to assess the timing performance of an individual FPGA, it is important for circuits whose timing must interact in complex ways with external inputs to assess the ability of the circuit as a whole to perform with variable clock rates, skews, and asymmetries. Recommend a test whereby the clock signals are run from an external function generator and rise time, frequency, and symmetry are adjusted over approximately a 10% range. (This can be accomplished by having the crystal oscillator connected to the rest of the system via a jumper wire.) This test, much like the Voltage Margin test, establishes that the design has adequate margin against both external and internal signal degradation due to aging effects.

POWER INTERFACES

INSTRUMENT INTERFACES:

P-1 IDPU Converted Power to FGM
P-1.1 FGM Sensor Power
P-1.2 FGM Boom Power

P-2 IDPU Converted Power to SCM
P-2.1 SCM Sensor Power
P-2.2 SCM Boom Power

P-3 IDPU Converted Power to EFI
P-3.1 EFI Sensor Power
P-3.2 EFI Radial Door Power
P-3.3 EFI Radial Motor Power
P-3.4 EFI Axial Boom Power

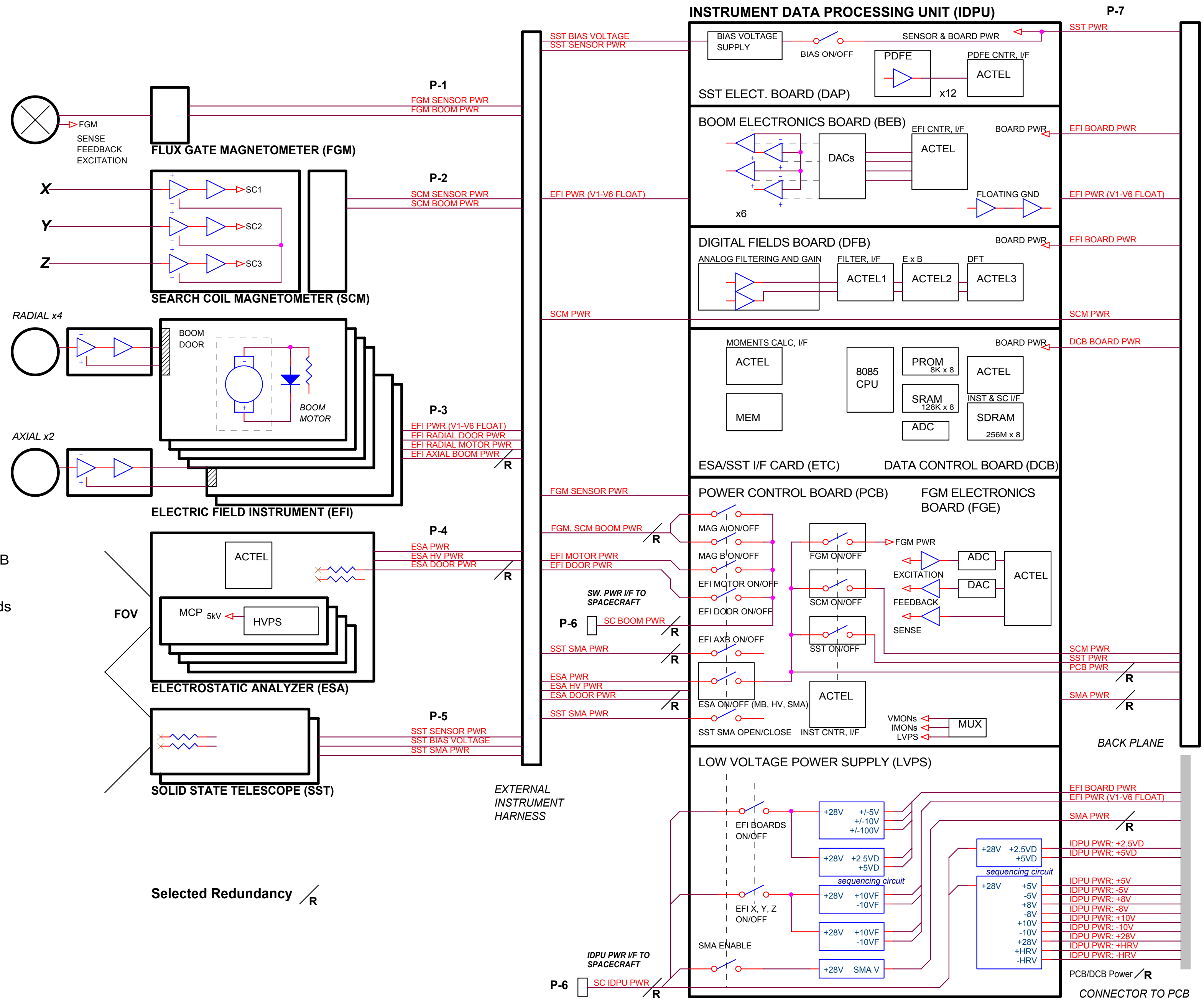
P-4 IDPU Converted Power to ESA
P-4.1 ESA LV Power
P-4.2 ESA HV Power
P-4.3 ESA Door Power

P-5 IDPU Converted Power to SST
P-5.1 SST Sensor Power
P-5.2 SST Bias Voltage Power
P-5.3 SST SMA Power

IDPU INTERFACES:

P-6 BAU Power to IDPU
P-6.1 BAU +28V Power to IDPU LVPS
P-6.2 BAU +28V Actuator Power to IDPU PCB
P-6.3 BAU Heater Power to IDPU PCB

P-7 IDPU Converted Power to all IDPU Boards
P-7.1 SST Board Power
P-7.2 EFI (DFB and BEB) Board Power
P-7.3 DCB Board Power
P-7.4 PCB Board Power



Title	THEMIS FMECA: POWER INTERFACES
Size	Document Number THM_SYS_007 APPENDIX A — Rev A
Date:	Sheet 1 of 1

DATA INTERFACES

INSTRUMENT INTERFACES:

D-1 FGM Data to IDPU
D-1.1 FGM Sense Data
D-1.2 FGM Feedback Data
D-1.3 FGM Excitation
D-1.4 FGM Housekeeping from Sensor
D-1.5 FGM High Speed Telemetry (128Hz)
D-1.6 FGM Lo Speed Telemetry (4-32Hz)
D-1.7 FGM/PCB Analog HK (AHK)
D-1.8 FGM Command (CMD)
D-1.9 FGM Synch (1PPS)

D-2 SCM Data to IDPU
D-2.1 SCM Calibration Signal
D-2.2 SCM Sensor Data (X,Y,Z)

D-3 EFI Data to IDPU
D-3.1 EFI Boom Analog HK (Turns Count)
D-3.2 EFI Control (Bias, Usher, Guard, Braid)
D-3.3 EFI Test Signal
D-3.4 EFI Telemetry (TLM)
D-3.5 EFI (BEB) Analog HK (AHK)
D-3.6 EFI Command (CMD)
D-3.7 EFI Synch (1PPS)

D-4 ESA Data to IDPU
D-4.1 ESA Telemetry (TLM)
D-4.2 ESA Analog HK (AHK)
D-4.2 ESA Command (CMD)
D-4.3 ESA Synch (Sun Pulse)

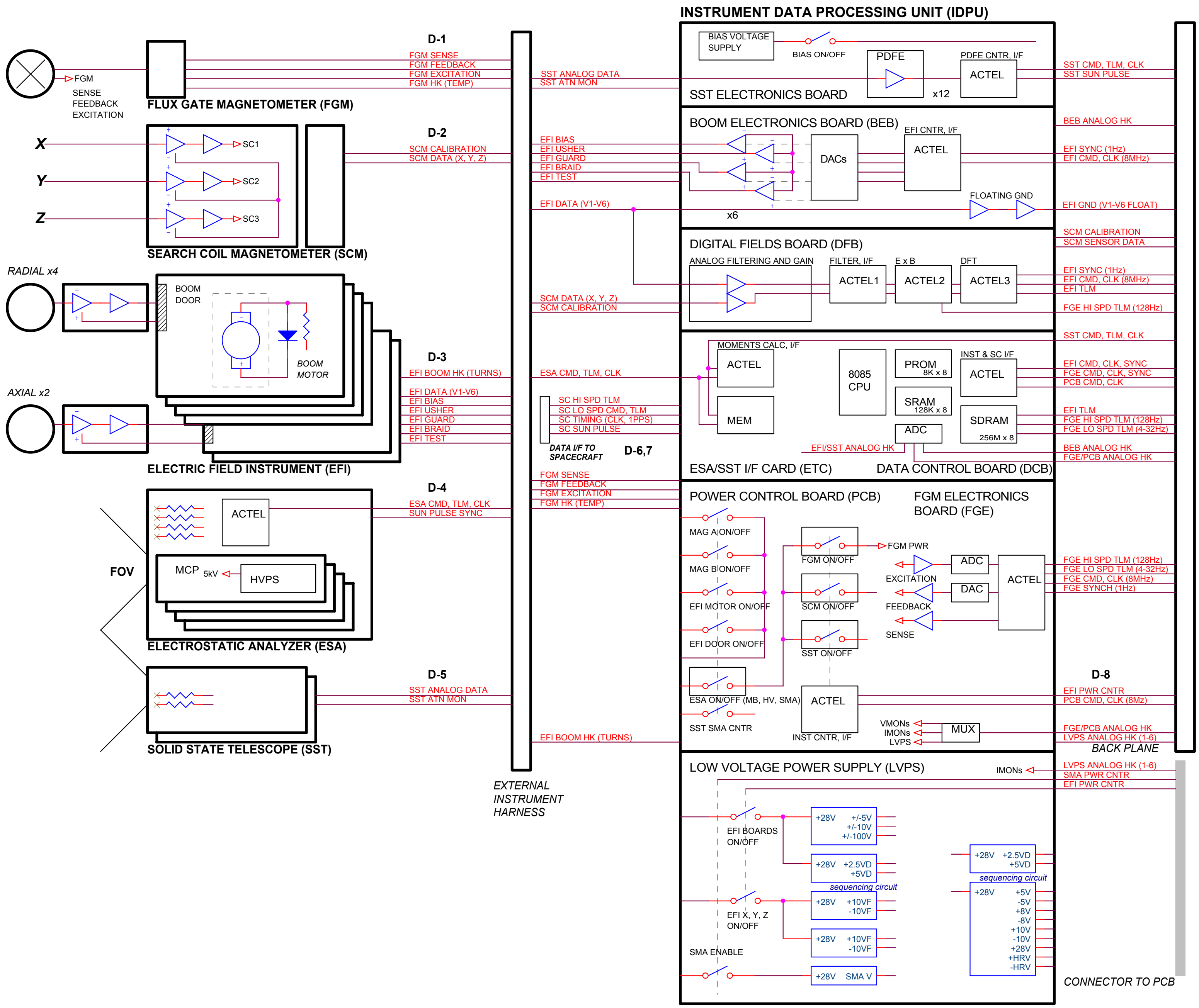
D-5 SST Data to IDPU
D-5.1 SST Analog Sensor Data
D-5.2 SST Attenuator Monitor
D-5.3 SST Telemetry (TLM)
D-5.4 SST Analog HK (AHK)
D-5.5 SST Command (CMD)
D-5.6 SST Synch (Sun Pulse)

IDPU INTERFACES:

D-6 IDPU Data to BAU
D-6.1 IDPU Data, high rate, to BAU
D-6.2 IDPU Data, low rate, to BAU

D-7 IDPU Command/Timing from BAU
D-7.1 BAU Command to IDPU
D-7.2 BAU Clock (8MHz) to IDPU
D-7.3 BAU Synch (1PPS) to IDPU
D-7.4 BAU Sun Pulse to IDPU

D-8 IDPU Core System (DCB, PCB, LVPS)
D-8.1 PCB/FGE Analog HK (AHK)
D-8.2 PCB Command (CMD)
D-8.3 PCB Synch (1PPS)
D-8.4 PCB EFI Power Control
D-8.5 PCB SMA Power Control
D-8.6 LVPS Analog HK (AHK)



Title	THEMIS FMECA: DATA INTERFACES	
Size	Document Number THM_SYS_007 APPENDIX A	Rev A
Date:	Sheet 1 of 1	

System	THEMIS		Prepared By	Ellen R. Taylor
Function	Power		FMEA Date	10/30/2003
Component	All		Revision Date	5/4/2004
Design Lead	Peter Berg			

Failure Mode Effects and Criticality Analysis
(Design FMECA)

ID	Interface	Potential Failure Mode(s)	Potential Effect(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Probability	Current Design Controls	Detectability	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
INSTRUMENT INTERFACES																
P-1 IDPU Converted Power to FGM																
P-1.1	FGM Sensor Power	1. No Voltage 2. Under-Voltage	No FGM data. Degraded science mission	High	Connector, Harness, Backplane, FET, FPGA control	Remote: Failure is unlikely	High Rel FETs, QA Harness	Very High	14	N/A						
P-1.2	FGM Boom Power	1. No Voltage 2. Under-Voltage	Boom doesn't deploy. FGM degraded due to close proximity to probe. Degraded science mission	High	Connector, Harness, Backplane, FET, Mechanism, Frangi-bolt actuator	Low-Moderate	High Rel FETs, QA Harness, Mechanism Testing	Very High	56	Add Redundancy for Mag Booms	October 2003, before design is final	Added Redundant FET to PCB, Redundant Wires	Hig	Ren	Ver	14
P-2 IDPU Converted Power to SCM																
P-2.1	SCM Sensor Power	1. No Voltage 2. Under-Voltage	No SCM data. Degraded science mission - SCM not critical for minimum mission.	Moderate	Connector, Harness, Backplane, FET, FPGA control	Remote: Failure is unlikely	High Rel FETs, QA Harness	Very High	12	N/A						
P-2.2	SCM Boom Power	1. No Voltage 2. Under-Voltage	Boom doesn't deploy. SCM unusable due to damage from thruster plume. Degraded science mission	High	Connector, Harness, Backplane, FET, Mechanism, Frangi-bolt actuator	Low-Moderate	High Rel FETs, QA Harness, Mechanism Testing	Very High	56	Add Redundancy for Mag Booms	October 2003, before design is final	Added Redundant FET to PCB, Redundant Wires	Hig	Ren	Ver	14
P-3 IDPU Converted Power to EFI																
P-3.1	EFI Sensor Power	1. No Voltage 2. Under-Voltage	No EFI data from one sensors. 6 sensors provide some redundancy. Degraded science mission	Moderate	Connector, Harness, Backplane, FET, FPGA control	Remote-Low	High Rel FETs, QA Harness	Almost Certain	12	N/A						
P-3.2	EFI Radial Door Power	1. No Voltage 2. Under-Voltage	Cannot deploy one wire boom. No EFI data from sensors. 4 sensors provide some redundancy. Degraded science mission. Stability OK with one failed SPB.	Moderate	Connector, Harness, Backplane, FET, Mechanism, SMA actuator	Low-Moderate	High Rel FETs, QA Harness, Mechanism Testing	Almost Certain	24	Add Redundancy in Door Mechanism	October 2003, before design is final	Added Redundant SMA Wire	Hig	Ren	Ver	14
P-3.3	EFI Radial Motor Power	1. No Voltage 2. Under-Voltage	Cannot fully deploy one wire boom. No EFI data from sensors. 4 sensors provide some redundancy. Degraded science mission. Stability OK with one failed SPB.	Moderate	Connector, Harness, Backplane, FET, Motors	Remote-Low	High Rel FETs, QA Harness	Almost Certain	12	N/A						
P-3.4	EFI Axial Boom Power	1. No Voltage 2. Under-Voltage	Cannot fully deploy axial boom. No EFI data from sensor. Degraded science mission. Axial Boom Sensor not critical to minimum science. Stability OK with one failed AXB.	Moderate	Connector, Harness, Backplane, FET, Mechanism, Frangi-bolt actuator	Low-Moderate	High Rel FETs, QA Harness, Mechanism Testing	Almost Certain	24	Add Redundancy for Axial Booms	October 2003, before design is final	Added Redundant FET to PCB, Redundant Wires	Hig	Ren	Alm	7
P-4 IDPU Converted Power to ESA																
P-4.1	ESA LV Power	1. No Voltage 2. Under-Voltage	No ESA data. Degraded science mission - ESA not critical for minimum science.	Moderate	Connector, Harness, Backplane, FET	Remote-Low	High Rel FETs, QA Harness	Almost Certain	12	N/A						
P-4.2	ESA HV Power	1. No Voltage 2. Under-Voltage	Poor quality ESA data. Degraded science mission	Moderate	Connector, Harness, Backplane, FET	Remote-Low	High Rel FETs, QA Harness	Almost Certain	12	N/A						
P-4.3	ESA Door Power	1. No Voltage 2. Under-Voltage	No ESA data if Door doesn't open. Degraded science mission.	Moderate	Connector, Harness, Backplane, FET, Mechanism, SMA actuator	Low-Moderate	High Rel FETs, QA Harness, Mechanism Testing	Almost Certain	24	Add Redundancy for EFI Door	October 2003, before design is final	Added Redundant FET to PCB, Redundant Wires	Hig	Ren	Ver	14
P-5 IDPU Converted Power to SST																
P-5.1	SST Sensor Power	1. No Voltage 2. Under-Voltage	No SST data from 1 SST. Degraded science mission	Moderate	Connector, Harness, Backplane, FET	Remote-Low	High Rel FETs, QA Harness	Almost Certain	12	N/A						
P-5.2	SST Bias Voltage Power	1. No Voltage 2. Under-Voltage	Poor SST data. Degraded science mission	Moderate	Connector, Harness, Backplane, FET	Remote-Low	High Rel FETs, QA Harness	Almost Certain	12	N/A						
P-5.3	SST SMA Power	1. No Voltage 2. Under-Voltage	Attenuated or non-attenuated SST data only. Slightly degraded science mission	Moderate	Connector, Harness, Backplane, FET, Mechanism, SMA actuator	Low-Moderate	High Rel FETs, QA Harness	Almost Certain	24	Parts Stress Analysis (PSA) on FETs	Aug 2004, before flight build					
IDPU INTERFACES																
P-6 BAU Power to IDPU																
P-6.1	BAU 28V to IDPU	1. No Voltage 2. Under-Voltage	No Instrument Power. Severely degraded science mission	Very High	Connector, Harness, BAU FET	Low: Relatively few failures	High Rel FETs, QA Harness	Almost Certain	24	Add Redundancy	October 2003, before final BAU-to-IDPU ICD	Redundant Wires added to Harness	Hig	Ren	Ver	14
P-6.2	BAU Actuator 28V to IDPU	1. No Voltage 2. Under-Voltage	No Instrument deployables. Severely degraded science mission	Very High	Connector, Harness, BAU FET	Low: Relatively few failures	High Rel FETs, QA Harness	Almost Certain	24	Add Redundancy	October 2003, before final BAU-to-IDPU ICD	Redundant Wires added to Harness	Hig	Ren	Ver	14
P-6.3	BAU Heater Power 28V to IDPU	1. No Voltage 2. Under-Voltage	No heater power to instruments, possible problems with electronics due to being too cold.	Low	Connector, Harness, BAU FET	Remote-Low	High Rel FETs, QA Harness	Almost Certain	10	N/A						

System	THEMIS	Prepared By	Ellen R. Taylor
Function	Power	FMEA Date	10/30/2003
Component	All	Revision Date	5/4/2004
Design Lead	Peter Berg		

Failure Mode Effects and Criticality Analysis
(Design FMECA)

ID	Interface	Potential Failure Mode(s)	Potential Effect(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Probability	Current Design Controls	Detectability	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
P-7 IDPU Converted Power to all IDPU Boards																
P-7.1	SST Board Power	1. No Voltage 2. Under-Voltage	No SST Data. Severely degraded science mission	High	Connector, Harness, BAU FET	Low: Relatively few failures	High Rel FETs, QA Harness	Almost Certain	21	Add Redundancy	October 2003, before design is final	Redundant pwr lines in LVPS connector and on Backplane to PCB added	Hig	Ren	Ver	14
P-7.2	EFI (DFB and BEB) Board Power	1. No Voltage 2. Under-Voltage	No EFI Data. Severely degraded science mission	High	Connector, Harness, BAU FET	Low: Relatively few failures	High Rel FETs, QA Harness	Almost Certain	21	Add Redundancy	October 2003, before design is final	Redundant pwr lines in LVPS connector and on Backplane to PCB added	Hig	Ren	Ver	14
P-7.3	DCB Board Power	1. No Voltage 2. Under-Voltage	No Instrument Data. Severely degraded science mission	Very High	Connector, Harness, BAU FET	Low: Relatively few failures	High Rel FETs, QA Harness	Almost Certain	24	Add Redundancy	October 2003, before design is final	Redundant pwr lines in LVPS connector and on Backplane to PCB added	Hig	Ren	Ver	14
P-7.4	PCB Board Power	1. No Voltage 2. Under-Voltage	No Instrument Data. Severely degraded science mission	Very High	Connector, Harness, BAU FET	Low: Relatively few failures	High Rel FETs, QA Harness	Almost Certain	24	Add Redundancy	October 2003, before design is final	Redundant pwr lines in LVPS connector and on Backplane to PCB added	Hig	Ren	Ver	14

System	THEMIS
Function	Data
Component	All
Design Lead	Dorothy Gordon

Failure Mode Effects and Criticality Analysis
(Design FMECA)

Prepared By	Ellen R. Taylor
FMEA Date	10/30/2003
Revision Date	5/4/2004

ID	Interface	Potential Failure Mode(s)	Potential Effect(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Probability	Current Design Controls	Detectability	R P N	Recommended Action(s)	Responsibility & Target Completion Date	Action Results				
												Actions Taken	New Sev	New Occ	New Det	New RPN
INSTRUMENT INTERFACES																
D-1 FGM Data to IDPU																
D-1.1	FGM Sense Data	1. No Data 2. Corrupted Data	No FGM data. Degraded science mission	High	Connector, Harness, FGE FPGA	Remote-Low	High Rel FPGA, FPGA Testing, QA Harness	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-1.2	FGM Feedback Data	1. No Data 2. Corrupted Data	No FGM data. Degraded science mission	High	Sensor failure, Connector, Harness, FGE DAC, FPGA	Remote-Low	High Rel FPGA, DAC, FPGA Testing, QA Harness	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-1.3	FGM Excitation	1. No Data 2. Corrupted Data	No FGM data. Degraded science mission	High	Sensor failure, Connector, Harness, FGE ADC, FPGA	Remote-Low	High Rel FPGA, ADC, FPGA Testing, QA Harness	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-1.4	FGM Housekeeping from Sensor	1. No Data 2. Corrupted Data	No FGM temperature data. Minor impact	Minor	Thermistor failure, Connector, Harness	Remote-Low	QA Harness	Very High	12	N/A						
D-1.5	FGM High Speed Telemetry (128Hz)	1. No Data 2. Corrupted Data	No Hi Speed FGM data. Low impact, redundant with low speed.	Very Low	FPGA, Backplane, SDRAM, 8085	Remote-Low	High Rel FPGA, FPGA Testing, 8085 Rad Hard	Very High	16	N/A						
D-1.6	FGM Lo Speed Telemetry (4-32Hz)	1. No Data 2. Corrupted Data	No Lo Speed FGM data. Minor impact, redundant with high speed.	Minor	FPGA, Backplane, SDRAM, 8085	Remote-Low	High Rel FPGA, FPGA Testing, 8085 Rad Hard	Very High	12	N/A						
D-1.7	FGM/PCB Analog HK (AHK)	1. No Data 2. Corrupted Data	HK only. No impact.	None	PCB MUX, Backplane, DCB ADC, 8085	Remote-Low	High Rel ADC, MUX, FPGA Testing, 8085 Rad Hard	Very High	4	N/A						
D-1.8	FGM Command (CMD)	1. No Command 2. Corrupted Command	Command required to start FGM data. No FGM data. Degraded science mission	High	8085, DCB FPGA, Backplane, FGE FPGA	Remote-Low	High Rel FPGA, FPGA Testing	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-1.9	FGM Synch (1PPS)	1. No Synch 2. Intermittent Synch	No FGM data. Degraded science mission	High	DCB FPGA, Backplane, FGE FPGA	Remote-Low	High Rel FPGA, FPGA Testing, Internal Synch	Very High	28	Add internal synch	April 2004, before FPGA design is final	Added internal synch pulse in FGE FPGA	Higl	Ren	Very	14
D-2 SCM Data to IDPU																
D-2.1	SCM Calibration Signal	1. No Data 2. Corrupted Data	Calibration increases quality of data. Minor impact.	Minor	8085, Backplane, Connector, Harness, Pre-Amp failure	Remote-Low	QA Harness	Very High	12	N/A						
D-2.2	SCM Sensor Data (X,Y,Z)	1. No Data 2. Corrupted Data	No SCM data. Degraded science mission, not critical instrument for minimum mission.	Moderate	Sensor failure, Connector, Harness, DFB Actels, Backplane, SDRAM, 8085	Remote-Low	High Rel FPGA, FPGA Testing, QA Harness	Very High	24	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-3 EFI Data to IDPU																
D-3.1	EFI Boom Analog HK (Turns Count)	1. No Data 2. Corrupted Data	Boom length can be determined without turns count. Minor impact.	Very Minor	Boom unit, Connector, Harness, PCB FPGA, PCB Mux, Backplane, DCB ADC, 8085	Remote-Low	High Rel Parts, Testing, QA Harness	Almost Certain	4	N/A						
D-3.2	EFI Control (Bias, Usher, Guard, Braid)	1. No Control 2. Corrupted Control	Cannot optimize for data quality. Low impact.	Low	8085, DCB FPGA, Backplane, BEB FPGA, BEB DACs, Connector, Harness	Remote-Low	High Rel Parts, Testing, QA Harness	Almost Certain	10	N/A						
D-3.3	EFI Test Signal	1. No Data 2. Corrupted Data	Used mainly for ground testing. No impact.	None	8085, DCB FPGA, Backplane, BEB FPGA, BEB DACs, Connector, Harness	Remote-Low	High Rel Parts, Testing, QA Harness	Very High	4	N/A						
D-3.4	EFI Telemetry (TLM)	1. No Data 2. Corrupted Data	No EFI data. Degraded science mission	High	Sensor, Pre-Amp, Connector, Harness, DFB FPGA, Backplane, SDRAM, 8085	Remote-Low	High Rel Parts, Testing, QA Harness	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-3.5	EFI (BEB) Analog HK (AHK)	1. No Data 2. Corrupted Data	DAC readback only. Commanded values known. No impact.	Very Minor	BEB Mux, Backplane, DCB ADC, 8085	Remote-Low	High Rel Parts, Testing	Very High	8	N/A						
D-3.6	EFI Command (CMD)	1. No Command 2. Corrupted Command	Cannot optimize for data quality. Minor impact.	Minor	8085, DCB FPGA, Backplane, DFB FPGA	Remote-Low	High Rel Parts, Testing	Very High	12	N/A						
D-3.7	EFI Synch (1PPS)	1. No Synch 2. Intermittent Synch	Required for Data to be obtained by DFB. Degraded Science Mission.	High	DCB FPGA, Backplane, DFB FPGA	Remote-Low	High Rel FPGA, FPGA Testing	Almost Certain	14	N/A						

System	THEMIS			Prepared By	Ellen R. Taylor
Function	Data			FMEA Date	10/30/2003
Component	All			Revision Date	5/4/2004
Design Lead	Dorothy Gordon				

Failure Mode Effects and Criticality Analysis
(Design FMECA)

Page 1 of 1

ID	Interface	Potential Failure Mode(s)	Potential Effect(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Probability	Current Design Controls	Detectability	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
D-4 ESA Data to IDPU																
D-4.1	ESA Telemetry (TLM)	1. No Data 2. Corrupted Data	No ESA data. Degraded science mission - ESA not critical for minimum mission.	Moderate	Sensor, Connector, Harness, ETC FPGA, SDRAM, 8085	Remote-Low	High Rel Parts, Testing, QA Harness	Very High	24	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-4.2	ESA Analog HK (AHK)	1. No Data 2. Corrupted Data	HV setting. Minor impact.	Minor	Sensor, Connector, Harness, Backplane, FPGA, 8085 Failure	Remote-Low	High Rel Parts, Testing, QA Harness	Very High	12	N/A						
D-4.3	ESA Command (CMD)	1. No Command 2. Corrupted Command	Required for Data. Degraded Science Mission.	Moderate	8085, DCB FPGA, Backplane, ETC FPGA, ESA FPGAs	Remote-Low	High Rel Parts, Testing, QA Harness	Almost Certain	12	N/A						
P-7.1	ESA Synch (Sun Pulse)	1. No Synch 2. Intermittent Synch	Required for Data. Degraded Science Mission.	Moderate	DCB FPGA, ETC FPGA	Remote-Low	High Rel FPGA, FPGA Testing	Almost Certain	12	N/A						
P-7.2																
P-7.3	SST Analog Sensor Data	1. No Data 2. Corrupted Data	No SST data. SST1 and SST2 provide some redundancy and science overlap. Slightly degraded science mission	Moderate	Sensor DFE, Connector, Harness, DAP PDFE	Remote-Low	High Rel Parts, Testing, QA Harness	Almost Certain	12	N/A						
P-7.4	SST Attenuator Monitor	1. No Data 2. Corrupted Data	Commanded value known, science data gives other indication. No impact.	None	Mechanism unit, Connector, Harness, DAP FPGA, 8085	Remote-Low	High Rel Parts, Testing, QA Harness	Very High	4	N/A						
D-5.3	SST Telemetry (TLM)	1. No Data 2. Corrupted Data	TLM is from SST1 and SST2 (no redundancy on this line). Degraded science mission	High	DAP FPGA, Backplane, ETC FPGA, 8085 Failure	Remote-Low	High Rel Parts, Testing, QA Harness	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-5.4	SST Analog HK (AHK)	1. No Data 2. Corrupted Data	Voltage and Temp monitors only. No impact.	None	DAP MUX, Backplane, DCB DAC, 8085 Failure	Remote-Low	High Rel Parts, Testing	Very High	4	N/A						
D-5.5	SST Command (CMD)	1. No Command 2. Corrupted Command	Required for optimizing data quaility. Slightly degraded science mission	Moderate	8085, DCB FPGA, Backplane, ETC FPGA, DAP FPGA	Remote-Low	High Rel FPGA, FPGA Testing	Almost Certain	12	N/A						
D-5.6	SST Synch (Sun Pulse)	1. No Synch 2. Intermittent Synch	Required for Data. Degraded Science Mission.	High	DCB FPGA, ETC FPGA	Remote-Low	High Rel FPGA, FPGA Testing	Almost Certain	14	N/A						
IDPU INTERFACES																
D-6 IDPU Data to BAU																
D-6.1	IDPU Data, high rate, to BAU	1. No Data 2. Corrupted Data	All Instrument Data. Could affect minimum mission	Very High	8085, Driver, Connector, Harness	Remote-Low	High Rel Parts, Differential Signals, QA Harness	Very High	32	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-6.2	IDPU Data, low rate, to BAU	1. No Data 2. Corrupted Data	HK and redundant science. Low impact.	Low	8085, RS-422 Driver/Reciever, Connector, Harness	Remote-Low	High Rel Parts, Differential Signals, QA Harness	Almost Certain	10	N/A						
D-7 IDPU Command/Timing from BAU																
D-7.1	BAU Command to IDPU	1. No Data 2. Corrupted Data	Not required for data send. Various impacts depending on mission phase.	Moderate	8085, RS-422 Driver/Reciever, Connector, Harness	Remote-Low	High Rel Parts, Differential Signals, QA Harness	Very High	24	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-7.2	BAU Clock (8MHz) to IDPU	1. No Clock 2. Intermittent Clock	Required for all instrument data. Could affect minimum mission	Very High	8085, RS-422 Driver/Reciever, Connector, Harness	Remote-Low	High Rel Parts, Differential Signals, QA Harness	Very High	32	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-7.3	BAU Synch (1PPS) to IDPU	1. No Synch 2. Intermittent Synch	No Instrument Data. Could affect minimum mission	Very High	DCB FPGA, RS-422 Driver/Reciever, Connector, Harness	Remote-Low	High Rel Parts, Differential Signals, Internal 1PPS Synch, QA Harness	Very High	32	Add internal synch	April 2004, before FPGA design is final	Added internal synch pulse on DCB	High	Rem	Very	14
D-7.3	BAU Sun Synch Pulse to IDPU	1. No Synch 2. Intermittent Synch	Internal IDPU sun synch available. Minor impact.	Minor	8085, DCB FPGA, RS-422 Driver/Reciever, Connector, Harness	Remote-Low	High Rel Parts, Internal Sun Synch, QA Harness	Very High	12	N/A						

System THEMIS
Function Data
Component All
Design Lead Dorothy Gordon

Failure Mode Effects and Criticality Analysis (Design FMECA)

Prepared By Ellen R. Taylor
FMEA Date 10/30/2003
Revision Date 5/4/2004

ID	Interface	Potential Failure Mode(s)	Potential Effect(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Probability	Current Design Controls	Detectability	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
D-8 IDPU Core System (DCB, PCB, LVPS)																
D-8.1	PCB/FGE Analog HK (AHK)	1. No Data 2. Corrupted Data	HK only. No impact.	None	PCB MUX, Backplane, DCB ADC, 8085	Remote-Low	High Rel Parts, Testing	Very High	4	N/A						
D-8.2	PCB Command (CMD)	1. No Command 2. Corrupted Command	PCB controls power to all instruments. Could be high impact.	High	8085, DCB FPGA, Backplane, ETC FPGA, PCB FPGA	Remote-Low	High Rel FPGA, FPGA Testing	Very High	28	FPGA Worst Case Analysis (WCA), Timing Analysis, Design Review	Aug 2004, before flight build					
D-8.3	PCB Synch (1PPS)	1. No Synch 2. Intermittent Synch	Required for commanding. Could be high impact.	High	DCB FPGA, Backplane, PCB FPGA	Remote-Low	High Rel Parts, Testing	Almost Certain	14	N/A						
D-8.4	PCB EFI Power Control	1. No Data 2. Corrupted Data	No EFI data. Degraded science mission	High	8085, PCB FPGA, FET	Remote-Low	High Rel Parts, Testing	Almost Certain	14	N/A						
D-8.5	PCB SMA Power Control	1. No Control	Affects ability to open ESA door, SST attenuators. Degraded science mission	Moderate	8085, PCB FPGA, FET	Remote-Low	High Rel Parts, Testing	Almost Certain	12	N/A						
D-8.6	LVPS Analog HK (AHK)	1. No Data 2. Corrupted Data	HK only. No impact.	None	LVPS Connector, PCB MUX, Backplane, DCB ADC, 8085	Remote-Low	High Rel Parts, Testing	Almost Certain	2	N/A						

Orig 5-Nov-03
Rev Orig

THEMIS COMPONENTS OUTLINE FOR PRA
INITIATING EVENT FAILURES AND SOME FAILURE EFFECTS
("MINI" FMEA)

1 ELECTRICAL POWER SUBSYSTEM
1.1 Solar Arrays
1.1.1 Top Panel
1.1.1.1 2 strings
Shorted cell: None (1)
Open cell: 50% loss of power during launch, contingency, thruster firings - Some restricted op's; Minor Loss of Mission Performance (2)
1.1.1.2 Coupling Diodes (2 for Top)
Shorted diode: None (1)
Open diode: 50% loss of power during launch, contingency, thruster firings - Some restricted op's; Minor Loss of Mission Performance (2)
1.1.2 Bottom Panel
1.1.2.1 2 strings
Shorted cell: None (1)
Open cell: 50% loss of power during launch, contingency, thruster firings - Some restricted op's; Minor Loss of Mission Performance (2)
1.1.2.2 Coupling Diodes (2 for Bottom)
Shorted diode: None (1)
Open diode: 50% loss of power during launch, contingency, thruster firings - Some restricted op's; Minor Loss of Mission Performance (2)
1.1.3 4 Side Panels
1.1.3.1 4 strings per side
Shorted cell: None (1)
Open cell: 1/16 loss of power during normal operations - Some restricted op's during max eclipse and EOL; Minor Loss of Mission Performance (2)
1.1.3.2 Coupling Diodes (1 per string)
Shorted diode: None (1)
Open diode: 1/16 loss of power during normal operations - Some restricted op's during max eclipse and EOL; Minor Loss of Mission Performance (2)
1.2 Battery
Battery Catastrophe Li-Ion batteries are dangerous and can explode - personnel or LV damage is possible - Cat (5) - This is a safety issue!
Single Cell Shorts: Bus voltage a bit low; slight risk to operating battery to higher Depth of Discharge - None (1)
A Cell Opens: No battery, not a problem until eclipse - Loss of Probe (4)
1.3 Battery Relay (BERB)
One shot operation, set to "Battery ON-Line" before launch.
Relay resets to "Battery OFF-Line" during mission:
No battery, not a problem until eclipse - Loss of Probe (4)

1.4 Shunt Regulation
1.4.1 Switched Shunts (Quan 3)
1.4.1.1 Shunt Transistor (1 per shunt)

Open: None (1)
Short: 25% loss of power during normal op's - Restricted op's during eclipse and EOL; Minor Loss of Mission Performance (2)

1.4.1.2 Coupling Diode (1 per shunt)

Short: None (1)
Open: 25% loss of power during normal op's - Restricted op's during eclipse and EOL; Minor Loss of Mission Performance (2)

1.4.1.3 Control Circuits

Circuit failure: Probable loss of power - Loss of Probe (4)

1.4.2 Linear Shunt Circuit (Quan 1), All components

Any failure: Loss of fine voltage regulation, bus voltage ripple excessive, possible degradation of science. Major Compromise of Probe Mission Usefulness (3)

1.5 Power Distribution
1.5.1 +28V Unswitched to Transponder

Open: Loss of Transponder - Loss of Probe (4)

1.5.2 +28V to IDPU

Open: Loss of science - Loss of Probe (4)

1.5.3 +28V to Heaters

Open: Loss of temp control during eclipse - Loss of Probe (4)

1.5.4 +28V to RCS Pressure Transducer

Open: None (1)

1.5.5 +28V to Instruments

One-time use for initial deployment of science instrument booms.
Open at initial usage: Loss of science - Loss of Probe (4)
Open at later time: None (1)

1.5.6 +28V to S/C Heaters

Open: Loss of temp control during eclipse - Loss of Probe (4)

1.5.7 +28V to Instrument Heaters

Open: Loss of temp control during eclipse - Loss of Probe (4)

1.5.8 +28V to RCS Heaters

Open: Loss of temp control during eclipse - Loss of Probe (4)

1.5.9 +28V Pulses to BERB

Not used after launch None (1)

1.5.10 +28V Pulses to RCS Latch Valves

One-shot usage after launch.
Fails to Operate: Loss of RCS - Loss of Probe (4)

1.5.11 +28V Pulses to RCS Thruster Valves

Thruster Failure to Operate
Thrusters T1 or T2: Loss of RCS - Loss of Probe (4)
Thrusters A1 or A2: Loss of Spin axis precession control. Major Compromise (3)

1.5.12 +28V Pulses to Pyro Arm
One-shot usage after launch.
Fails to Operate: No separation - Loss of Probe (4)

1.5.13 +28V Pulses to Pyro Fire
One-shot usage after launch.
Fails to Operate: No separation - Loss of Probe (4)

1.5.14 Power Distribution and LVPS +5V to Backplane
Fails to Operate: No power - Loss of Probe (4)

1.5.15 Power Distribution and LVPS +3.3V to Backplane
Fails to Operate: No power - Loss of Probe (4)

1.5.16 Power Distribution and LVPS +3.3V(2.5) to Backplane
Fails to Operate: No power - Loss of Probe (4)

1.5.17 Power Distribution and LVPS +/-15V to Backplane
Fails to Operate: No power - Loss of Probe (4)

1.5.18 Power Distribution and LVPS +/-5V to Gyros
Fails to Operate: No gyros - Possible work-around using Magnetometer. Major Compromise (3)

1.5.19 Power Distribution and LVPS +5V to Sun Sensor
Fails to Operate: No Sun Sensor - Major degradation, Possible work-around using Magnetometer at perigee, questionable operations. Major Compromise (3)

2 ATTITUDE CONTROL SUBSYSTEM

2.1 Sun Sensor

Fails to Operate: No Sun Sensor - Major degradation, Possible work-around using Magnetometer at perigee, questionable operations.
Major Compromise (3)

2.2 Solid State Gyros (Quan 2)

One Fails to Operate: Only one gyro - Work-around is clumsy.
Some Compromise (2)

Both Fail to Operate: No gyros - Possible work-around using Magnetometer.
Major Compromise (3)

2.3 3-Axis Magnetometer (FGM Instrument)

Fails to Operate: No Earth's magnetic vector data.
Science: Loss of Probe (4)
Attitude Control: Major degradation, Possible work-around using Sun Sensor, questionable operations - Major Compromise (3) (But Probe is useless anyway.)

2.4 Software Functions (Physically located on and executed by ColdFire Processor)

Fails to Operate: Loss of Probe (4)

3 REACTION CONTROL SUBSYSTEM

3.1 Software Functions

Fails to Operate: Can't thrust properly - Loss of Probe (4)

3.2 Tanks (Quan 2)

Either Leak, Rupture: Tanks cannot be isolated, loss of fuel - Loss of Probe (4)

3.3 Flight Pressure Transducer

Fails to Operate: No effect - None (1)

3.4 Thermistors

Fail to Operate: No effect - None (1)

3.5 PRTs

Fail to Operate: No effect - None (1)

3.6 Pressure/Vent Valve (Quan 1, Manual)

No Credible Failure: GSE ops only, no effect - None (1)

3.7 Fill/Drain Valve (Quan 1 per Tank, Manual)

No Credible Failure: GSE ops only, no effect - None (1)

3.8 System Filter (Quan 2)

Either Filter Clogs: Cannot access fuel from one Tank. Consequence to THEMIS mission depends upon what orbital position is occupied by the Probe with the clogged RCS filter. Orbits 1 and 2 (outer orbits) need both tanks of fuel to reach EOL. Orbits 3,4,5 (inner orbits) need only one tank of fuel to reach EOL. For outer orbits the Probe may not reach EOL.
Clogged Filter, Probes 1 or 2: Early in life, Major Compromise (3)
Clogged Filter, Probes 1 or 2: Late in life, Loss of Probe (4)
Clogged Filter, Probes 3,4, or 5: Early in life, Some Compromise (2)
Clogged Filter, Probes 3,4, or 5: Late in life, Major Compromise (3)

3.9 Latch Valve (Quan 2)

Valve Stuck Closed: Both Valves are normally Open during mission life. With a closed Latch Valve, cannot access fuel in one Tank. Consequence to THEMIS mission depends upon what orbital position is occupied by the Probe with the closed Latch Valve. Orbits 1 and 2 (outer orbits) need both tanks of fuel to reach EOL. Orbits 3,4,5 (inner orbits) need only one tank of fuel to reach EOL. For outer orbits the Probe may not reach EOL.
Valve Stuck Closed, Probes 1 or 2: Early in life, Major Compromise (3)
Valve Stuck Closed, Probes 1 or 2: Late in life, Loss of Probe (4)
Valve Stuck Closed, Probes 3,4, or 5: Early in life, Some Compromise (2)
Valve Stuck Closed, Probes 3,4, or 5: Late in life, Major Compromise (3)

3.10 Orifice (Quan 2)

No Credible Failure Mode

3.11 Lines

Fuel leak, Any Line Loss of Probe (4).

3.12 Line Heater Series Strings (Two series strings powered redundantly)

Loss of One Heater String Loss of redundancy, otherwise no effect - None (1).
Loss of Both Heater Strinc Line freezes during eclipse - Loss of Probe (4).

3.13 Tank Heaters (These are redundant)

Loss of One Heater String Loss of redundancy, otherwise no effect - None (1).
Loss of Both Heater Strinc Tank freezes during eclipse - Loss of Probe (4).

3.14 Thruster Heaters (These are redundant, 2 per Thruster)

Loss of One Heater Loss of redundancy, otherwise no effect - None (1).
Loss of Both Heaters Thruster freezes during eclipse; all four thrusters are required. Loss of Probe (4).

3.15 Thruster Valve (Quan 2 in series per Thruster)

Either But Not Both Valve Seats Stuck in "Firing" Position
Loss of redundancy, otherwise no effect - None (1).
Both Valve Seats Stuck in "Firing" Position
Thruster fires continuously - Loss of Probe (4).
Either Or Both Valve Seats Stuck in "Non-Fire" Position
Cannot use thruster - Loss of Probe (4).

3.16 CatBed Heater (These are redundant, 2 per CatBed)

Loss of One CatBed Heate Loss of redundancy, otherwise no effect - None (1).
Loss of Both CatBed Heat Cannot safely use thruster during eclipse - Loss of Probe (4).

4 COMMUNICATION SUBSYSTEM

4.1 Antenna

Fails to Operate: Loss of Probe (4)

4.2 Transponder

4.2.1 Receiver

Fails to Operate: Loss of Probe (4)

4.2.2 Transmitter

Fails to Operate: Loss of Probe (4)

4.2.3 Diplexer

Fails to Operate: Loss of Probe (4)

4.3 Uplink FPGA on Communications Board

Fails to Operate: Loss of Probe (4)
This FPGA contains the following functions:
Uplink Command Interface
Command Verification
Hardware Command Interface

4.4 Command FIFO (One Integrated Circuit Device)

Fails to Operate: Loss of Probe (4)

4.5 Discrete Command Generator (Part of Power Board FPGA)

Fails to Operate: Loss of Probe (4)

4.6 Separation Interface (Telemetry function only)

Fail to Operate: No effect - None (1)

4.7 Analog Telemetry Current Source

Fails to Operate: Loss of important telemetry - Severe degradation, Probe survival and usefulness questionable - Major Degradation (3)

4.8 Analog Telemetry Multiplexer

Fails to Operate: Loss of important telemetry - Severe degradation, Probe survival and usefulness questionable - Major Degradation (3)

4.9 Telemetry Processor (Part of Power Board FPGA)

Fails to Operate: Loss of important telemetry - Severe degradation, Probe survival and usefulness questionable - Major Degradation (3)

4.10 Telemetry FIFO (One Integrated Circuit Device)

Fails to Operate: Loss of entire downlink - Loss of Probe (4)

4.11 Reed-Solomon Encoder (One Integrated Circuit Device)

Fails to Operate: Loss of entire downlink - Loss of Probe (4)
(Recommend consideration of a bypass capability.)

4.12 Downlink FPGA on Communications Board

Fails to Operate: Loss of Probe (4)
This FPGA contains the following functions:
Convolutional Encoder
Downlink Telemetry Interface
(Recommend consideration of a Convolutional Encoder bypass capability.)

4.13 Software Functions (Physically located on and executed by ColdFire Processor)

Fails to Operate: Loss of Probe (4)

5 C&DH/PROCESSOR SUBSYSTEM

5.1 Clock Oscillator
Fails to Operate: Loss of Probe (4)

5.2 ColdFire Processor
Fails to Operate: Loss of Probe (4)

5.3 Processor FPGA
Fails to Operate: Loss of Probe (4)

5.4 RAM
Fails to Operate: Loss of Probe (4)

5.5 Boot PROM
Fails to Operate: Loss of Probe (4)

5.6 Program Storage EEPROM
Fails to Operate: Loss of Probe (4)

5.7 RS-422 Command Driver to IDPU
Fails to Operate: Loss of Probe (4)

5.8 RS-422 Status Receiver from IDPU
Fails to Operate: Probably not critical - Some Compromise (2)

5.9 RS-422 2Mbps Data Receiver from IDPU
Fails to Operate: Loss of Probe (4)

5.10 RS-422 Clock Interfaces to IDPU
Fails to Operate: Loss of Probe (4)

5.11 RS-422 One PPS Interfaces to IDPU
Fails to Operate: Loss of timing sync to IPDU - Degraded science, usefulness questionable - Major Degradation (3)

5.12 Sun Pulse Interface to IDPU
Fails to Operate: Loss of spinner sync to IPDU - Degraded science, usefulness questionable - Major Degradation (3)

5.13 3.3V Power Switch to EEPROMs
Fails Shorted: No effect other than increased power consumption - None (1)
Fails Open: Cannot re-load flight application software; no effect unless rebooting Some Compromise (2)

5.14 Bulk Memory
Fails to Operate: Loss of Probe (4)

5.15 Bulk Memory FPGA
Fails to Operate: Loss of Probe (4)

5.16 Software Functions (Physically located on and executed by ColdFire Processor)
Fails to Operate: Loss of Probe (4)

6 BACKPLANE

6.1 I^2C Interfaces (Quan 3)

Any Fails to Operate: Loss of Probe (4)

7 HARNESS AND GROUNDING

7.1 Pyro Arm Plug

No Credible Failure Plug with jumper wires installed before flight.

7.2 RCS Arm Plug

No Credible Failure Plug with jumper wires installed before flight.

7.3 Fusing (Steered Redundant) - for non-critical loads only

7.3.1 Gyro +/-5V power

One Fuse Fails Open: None (1)

Both Fuses Fail Open: No gyros - Possible work-around using Magnetometer. Major Compromise (3)

7.3.2 Bus heaters

One Fuse Fails Open: None (1)

Both Fuses Fail Open: Loss of temp control during eclipse. Loss of Probe (4)

7.3.3 RCS heaters

One Fuse Fails Open: None (1)

Both Fuses Fail Open: Loss of temp control during eclipse. Loss of Probe (4)

7.3.4 Instrument heaters

One Fuse Fails Open: None (1)

Both Fuses Fail Open: Loss of temp control during eclipse. Loss of Probe (4)

7.3.5 Pressure Transducer

One Fuse Fails Open: None (1)

Both Fuses Fail Open: Loss of RCS pressure tlm - None (1)

7.4 Primary Return wires

Wire Fails Open: Loss of power - Loss of Probe (4)

7.5 Secondary/Signal Return wires

Wire Fails Open: Loss of power and/or signal return - Loss of Probe (4)

7.6 Chassis Return wires

Wire Fails Open: Loss of chassis ground, ops probably okay except noisy, probable degradation of science - Some Compromise (2)

FAILURE SEVERITY (CONSEQUENCE) CATEGORIES

5 Death/Injury of One or More Personnel; Loss/Damage to Launch Vehicle

4 Complete Loss of Probe
(If this Probe is mission-critical; Loss of Minimum Mission)

3 Major Compromise of Probe Mission Usefulness
(If this Probe is mission-critical; Retention of Minimum Mission but Major Degradation of Mission Performance)

2 Some Compromise of Probe Mission Usefulness
(If this Probe is mission-critical; Minor Loss of Some Mission Performance)

1 No Effect upon Probe Mission Usefulness

FAILURE PROBABILITY (FREQUENCY) CATEGORIES
2 YEAR (17,520 HOURS) MISSION

LOG SCALE

4 $P(S) < 0.9000$
$P(F) > 0.1000$

3 $0.9000 \leq P(S) < 0.9900$
$0.1000 \geq P(F) > 0.0100$

2 $0.9900 \leq P(S) < 0.9990$
$0.0100 \geq P(F) > 0.0010$

1 $0.9990 \leq P(S) < 0.9999$
$0.0010 \geq P(F) > 0.0001$

6-Sep-2002
rep
Rev Orig

Estimated MTBF, FITs =	Solar Array	Battery	Power Control Electronics	Measure Attitude	Input Avionics	Receiver and Antenna	Receive Avionics	Proc Avionics	C&DH Software	Relay Actions	Angular and Translation Actuation	Collect Payload Data	Store Data		Transmit Avionics	Transmitter and Antenna
	100 (per array side)	100	800	300	600	2000 (Receive part of S-band xpnder)	400	600	100 (software, patchable, S/C safe until patch)	600	600	0 (payload "0" failure)	600	300	400	3000 (Xmit part of S-band xpnder)

(Based upon EO-1 Red Team estimates from TRW)

THEMIS 1 Year Mission Reliability: Maneuver and Science Mode Architecture (Limiting Case)

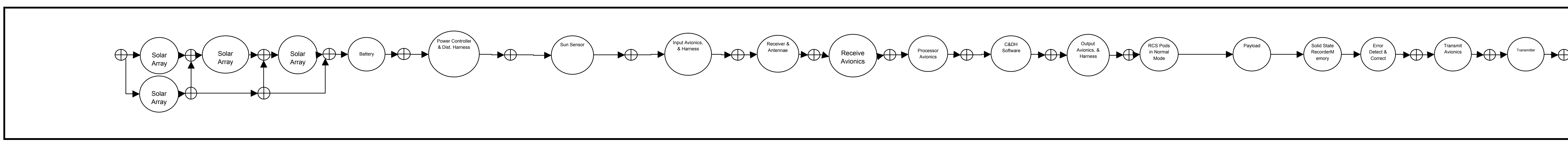
T, Years = 1
T, Hours = 8760

System Function	Power System: Solar Array	Power System: Battery	Power Control Electronics		Measure Attitude		Collect and Control-Critical Data: Input Avionics	Collect Command Instructions Regarding Target: Receiver and Antenna	Collect Command Instructions Regarding Target: Receive Avionics	Maneuver Control Processing: Proc Avionics	Maneuver Control Processing: C&DH Software	Relay Actions	Angular and Translation Actuation	Collect Payload Data	Store Data		Transmit Data: Transmit Avionics	Transmit Data: Transmitter and Antenna
Component Item	R_{SA}	R_{BAT}	R_{PCE}		R_{SS}		R_{IA}	R_{Rx}	R_{RA}	R_{PA}	R_{SW}	R_{OA}	R_{RCSpod}	$R_{Payload}$	R_{SSR}	R_{EDAC}	R_{TA}	R_{Tx}
Functional String Reliability	0.9991	0.9991	0.9930		0.9974		0.9948	0.9826	0.9965	0.9948	0.9991	0.9948	0.9948	1.0000	0.9948	0.9974	0.9965	0.9741
System Function Reliability	0.999995	0.9991	0.9930		0.9974		0.9948	0.9826	0.9965	0.9948	0.9991	0.9948	0.9895	1.0000	0.9948	0.9974	0.9965	0.9741
Satellite Reliability	**0.9081**																	

THEMIS 2 Year Mission Reliability: Maneuver and Science Mode Architecture (Limiting Case)

T, Years = 2
T, Hours = 17520

System Function	Power System: Solar Array	Power System: Battery	Power Control Electronics		Measure Attitude		Collect and Control-Critical Data: Input Avionics	Collect Command Instructions Regarding Target: Receiver and Antenna	Collect Command Instructions Regarding Target: Receive Avionics	Maneuver Control Processing: Proc Avionics	Maneuver Control Processing: C&DH Software	Relay Actions	Angular and Translation Actuation	Collect Payload Data	Store Data		Transmit Data: Transmit Avionics	Transmit Data: Transmitter and Antenna
Component Item	R_{SA}	R_{BAT}	R_{PCE}		R_{SS}		R_{IA}	R_{Rx}	R_{RA}	R_{PA}	R_{SW}	R_{OA}	R_{RCSpod}	$R_{Payload}$	R_{SSR}	R_{EDAC}	R_{TA}	R_{Tx}
Functional String Reliability	0.9982	0.9982	0.9861		0.9948		0.9895	0.9656	0.9930	0.9895	0.9982	0.9895	0.9895	1.0000	0.9895	0.9948	0.9930	0.9488
System Function Reliability	0.999982	0.9982	0.9861		0.9948		0.9895	0.9656	0.9930	0.9895	0.9982	0.9895	0.9792	1.0000	0.9895	0.9948	0.9930	0.9488
Satellite Reliability	**0.8247**																	



6-Sep-2002
rep
Rev Orig

THEMIS 1 YEAR MISSION RESULTS

Number of Total Probes in Constellation				5
		Ps (sat)	N	S
		0.908	4	1
Series Terms	4	0.312		
	5	0.618		
	6	#NUM!		
	7	#NUM!		
System Probability		0.930		

THEMIS 2 YEAR MISSION RESULTS

Number of Total Probes in Constellation				5
		Ps (sat)	N	S
		0.825	4	1
Series Terms	4	0.405		
	5	0.381		
	6	#NUM!		
	7	#NUM!		
System Probability		0.787		