RELIABILITY ANALYSIS OF SWAMPSAT

By

BUNGO SHIOTANI

A THESIS PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE

UNIVERSITY OF FLORIDA

2011

To my family, friends, and colleagues for all their support

ACKNOWLEDGEMENTS

First I would like to thank my family for their long support. Without them, I will not have had the privilege to study in the United States. Arigatou, kansha shitemasuwa.

I would also like to show my appreciation for my advisor and chair, Dr. Norman Fitz-Coy for all his knowledge and support. Not only was Dr. Fitz-Coy my advisor, he was a great mentor, always challenging my knowledge. His wisdom guided me in earning my Master of Science degree. To my committee members, Dr. John Schueller and Dr. Mrinal Kumar, I would like to express my gratitude for all your guidance and support.

To my fellow Space Systems Group members, thank you for always being there to help me get through. Without you guys, I would not have gotten this far. Lastly to all my friends all over the world, I want to let you guys know that I made it.

TABLE OF CONTENTS

page

CHAPTER

APPENDIX

LIST OF TABLES

Table page

LIST OF FIGURES

Figure page

LIST OF ABBREVIATIONS

ACS	Attitude Control System
ADC	Analog-to-Digital Converter
ADS	Attitude Determination System
CAC	CubeSat Acceptance Checklist
Cal Poly	California Polytechnic State University
CDH	Command and Data Handling
CDS	CubeSat Design Specification
CMG	Control Moment Gyroscope
CMG Ops	Control Moment Gyroscope Operations
Comms	Communications
COTS	Commercial Off-the-Shelf
DoD	Department of Defense
EEPROM	Electrically Erasable and Programmable Read-Only Memory
EKF	Extended Kalman Filtering
EPS	Electrical Power System
FAA	Federal Aviation Administration
FMECA	Failure Modes, Effects, and Criticality Analysis
FTA	Fault Tree Analysis
I2C	Inter-Integrated Circuit
ICD	Interface Control Document
IMU	Inertial Measuring Unit
ISS	International Space Station
LEO	Low Earth Orbit

LL	Level of Likelihood
LS	Level of Severity
LSP	Launch Service Provider
NASA	National Aeronautics and Space Administration
P-POD	Poly-Picosatellite Orbital Deployer
QUEST	Quaternion Estimator
R2P2	Rapid Retargeting and Precision Pointing
RBF	Remove Before Flight
RTC	Real Time Clock
SFC	SwampSat Flight Computer
SPI	Serial Peripheral Interface
SSDL	Space Systems Development Laboratory
SSG	Space Systems Group
TI-DSP	Texas Instruments – Digital Signal Processor
TT&C	Telemetry, Tracking and Command

Abstract of Thesis Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Master of Science

RELIABILITY ANALYSIS OF SWAMPSAT

By

Bungo Shiotani

August 2011

Chair: Norman G. Fitz-Coy
Major: Aerospace Engineering

SwampSat is a picosatellite designed and developed by the University of Florida to demonstrate rapid retargeting and precision pointing (R2P2) using four single gimbal control moment gyroscopes (CMGs). As part of the design and development of SwampSat, reliability analysis has been performed to identify and mitigate possible failures. In most applications, reliability information can be obtained by prior experiences, however, for SwampSat there is a lack of such information since it is the first of its kind. Two different techniques were used for the reliability analysis of SwampSat. The first technique used the Failure Modes, Effects, and Criticality Analysis (FMECA), which ranks the criticality for each failure mode and thus prioritizes the risks. Lower risks were ranked for space qualified components and higher risks were assigned for built in-house components. The second technique used the Fault Tree Analysis (FTA) to complement the FMECA by starting with a top-level failure effect and traces the failure to potential lowest level causes.

This thesis uses these two reliability analysis techniques to identify possible failures of SwampSat. With the possible failures identified, appropriate mitigation plans

and preventive actions were developed for the SwampSat mission, but these are beyond the scope of this effort.

CHAPTER 1
INTRODUCTION

1.1 Introduction to CubeSats

Small satellites have been extremely attractive in recent years. Traditional satellites require tremendous development time and enormous cost. Small satellites on the other hand, can demonstrate innovative technology with shorter development times and lower costs. Due to their reduced mass, the small satellites can be launched as secondary payloads. Small satellites are particularly suited for educational purposes and many universities all over the world have initiated small satellite research and development programs. Satellites that are considered as small satellites have masses less than 500 kg and the small satellites can be categorized into four classes according to their mass. Pico-satellites have mass of 1 kg or less, nano-satellites have mass of 10 kg or less, micro-satellites have mass of 100 kg or less and mini-satellites have mass of 500 kg or less.

The CubeSat program began as a collaborative effort between California Polytechnic State University (Cal Poly) and the Space Systems Development Laboratory (SSDL) at Stanford University. The objective of the CubeSat program is to provide a standard platform for the design and launch of a new class of pico-satellites – CubeSats. [1] The CubeSat standard specifies 1U CubeSats should be a 10 cm cube and a have maximum mass of 1 kg. The original CubeSat standard was developed from the size of the commercial off-the-shelf (COTS) components, the dimension and features of Poly-Picosatellite Orbital Deployer (P-POD) [2], launch vehicle environmental and operational requirements, and self-imposed safety standards [3]. Recently the new CubeSat Design Specification (CDS) has changed the maximum mass to 1.33 kg [4]. The 10 cm cube is also known as a 1U CubeSat form factor. CubeSats can also be designed as a 1U, 2U, or a 3U. A single P-POD can carry three 1U CubeSats or one 1U and one 2U, or one 3U CubeSats depending on what the designers decide. Different sizes for CubeSats create new challenges and opportunities for universities to research and develop innovative technology utilizing commercially available parts.

1.2 SwampSat Mission Objective

SwampSat is a 1U CubeSat developed by the Space Systems Group (SSG) at the University of Florida [5]. The objective of SwampSat is a flight validation of compact three-axis attitude control system capable of rapid retargeting and precision pointing (R2P2) for pico- and nano-satellite applications. To demonstrate the R2P2 task, four single gimbal control moment gyroscopes (CMG) in a tetrahedral pyramid configuration will be used [6]. The SwampSat is designed to operate in the low earth orbit (LEO). The SwampSat mission proposes to validate the following operations on orbit: (1) establish a communication link in both directions; (2) validate supporting subsystems, Attitude Determination System (ADS), Command and Data Handling (CDH), and Electrical Power System (EPS); (3) downlink pre-maneuver attitude data; (4) perform attitude maneuver, Sun pointing and retargeting; (5) downlink post-maneuver data and analysis of pre-and post-maneuver data to validate maneuvers.

The SwampSat mission profile shown in Figure 1-1 was created to validate the concept of operations. The SwampSat software is designed as operating modes and implemented as software tasks shown in Appendix A [7]. Using the SwampSat mission profile and the software architecture, reliability analysis for SwampSat was performed.

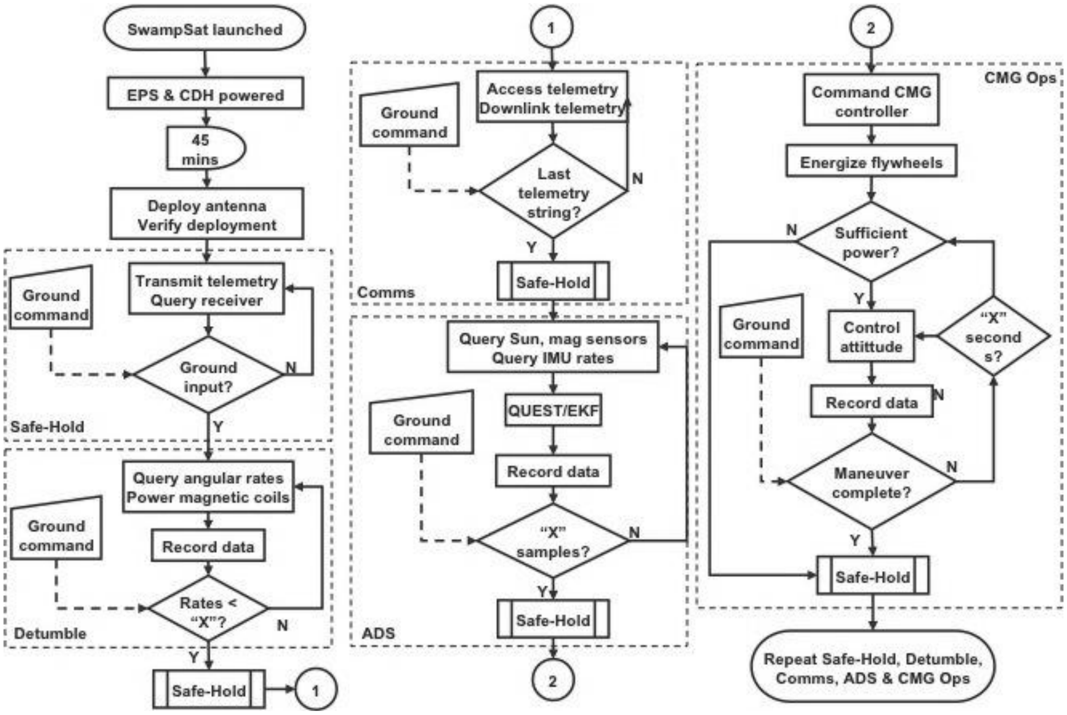


Figure 1-1. SwampSat mission profile

1.3 Motivation

Reliability analysis is a necessity for all projects. Fabio Santoni presented a paper on risk management for micro-satellite design at the 48th International Astronautical Congress in 1997 where he used the Failure, Modes, Effects, and Criticality Analysis (FMECA) as the risk analysis for the design of University of Rome micro-satellite [8]. It seems as though this paper is the only publication that includes the risk analysis for small satellites. There are many publications that have risk analysis for satellites but only a few for small satellites.

SwampSat is the first CubeSat developed by the University of Florida and by performing the reliability analysis, possible failures will be outlined. In most applications reliability data is available from previous and similar applications. For SwampSat, there is lack of data due an absence of flight heritage on some components, therefore, the analysis was a difficult task. Using two different reliability analyses for SwampSat, more failures will be identified which will allow for necessary mitigation plans to be created. Performing the Failure Modes, Effects, and Criticality Analysis (FMECA) first will determine the higher risks for SwampSat. Using those higher risks, Fault Tree Analysis (FTA) will be performed to identify the lower level failures associated with the higher risk items. Once both analyses are performed, necessary mitigation plans will be created for potential failures. In order for the SwampSat mission to be a success, all failures that can be identified must be addressed. Performing reliability analysis, FMECA and FTA, will greatly impact SwampSat mission success.

The thesis is organized as follows. Chapter 1 provides an introduction to small satellites, CubeSats, as well as SwampSat. Chapter 2 explores the two types of reliability analysis used for SwampSat. The SwampSat FMECA and SwampSat FTA are detailed in Chapter 3 and Chapter 4, respectively. Chapter 5 presents the conclusion and future work.

CHAPTER 2
RELIABILITY ANALYSIS

2.1 Introduction to Reliability Analysis

Reliability analysis is one of the most important steps in designing and developing complex systems defined as collection of different elements that together produce results not obtainable by the elements alone [9]. The primary aim of system reliability is the prevention of failures that affect the operational capability of a system [10]. Reliability is a characteristic of an item, expressed by the probability that the item will perform its required function under given conditions for a stated time interval. Performing reliability analysis will identify the sources of high risk failures in a complex system. Risk is defined as the combination of the probability that a program or project will experience an undesired event and the consequences, impact, or severity of the undesired event, were it to occur. Once the risks have been identified, the failures can be eliminated or reduced to some acceptable level that the designers of the project can agree to. Risk and reliability analysis are not limited to the beginning of the project but rather it is a continuing effort during the project. [9, 11] During the early stages in a project, reliability analysis can be used to understand and discover key relationships in the design so they can be properly considered. As the project advances, the reliability analysis can be used to thoroughly examine for any accident initiations and hazards that could lead to mishaps. During the latter phases, the reliability analysis can be used to verify that the design is meeting the goals and if the goals are not met then mitigation strategies can be developed.

The most commonly used analytical techniques for failure prevention are the Failure Modes, Effects, and Criticality Analysis (FMECA), and the Fault Tree Analysis

(FTA). Both FMECA and FTA are methodologies designed to identify potential failure modes for a product or process, to assess the risk associated with those failure modes, to rank the issues in terms of importance, and to identify and carry out corrective actions to address the most serious concerns [12, 13]. When changes are made in the system design to remove or reduce the impact of the identified failures, the FMECA and the FTA must be repeated for the redesigned parts to ensure that all the predictable failures in the new design are thoroughly considered.

2.2 Introduction to FMECA

FMECA is the foundation of all the other analysis techniques for reliability of a system [14]. For each failure mode, the effects are evaluated at the next system level and detection methods are listed. FMECA also include an evaluation of the criticality of the failure modes based upon the severity of the effect on the system and the likelihood of the occurrence. FMECA was originally developed by the National Aeronautics and Space Administration (NASA) to improve and verify the reliability of space program hardware. Now FMECA has been used by different agencies to identify failures. The Department of Defense (DoD) is one of the agencies that use FMECA for their projects. The DoD has created a document that explains the procedure of performing a FMECA. The document, MIL-STD-1629A states:

> the military standard that establishes requirements and procedures for performing a FMECA, to evaluate and document, by failure mode analysis, the potential impact of each functional or hardware failure on mission success, personal and system safety, maintainability and system performance. Each potential failure is ranked by the severity of its effect so that corrective actions may be taken to eliminate or control design risk. High risk items are those items whose failure would jeopardize the mission or endanger personnel. The techniques presented in this standard may be applied to any electrical or mechanical equipment or system. Although MIL-STD-1629A has been cancelled, its concepts should be applied during the

> development phases of all critical systems and equipment whether it is military, commercial or industrial systems/products [15].

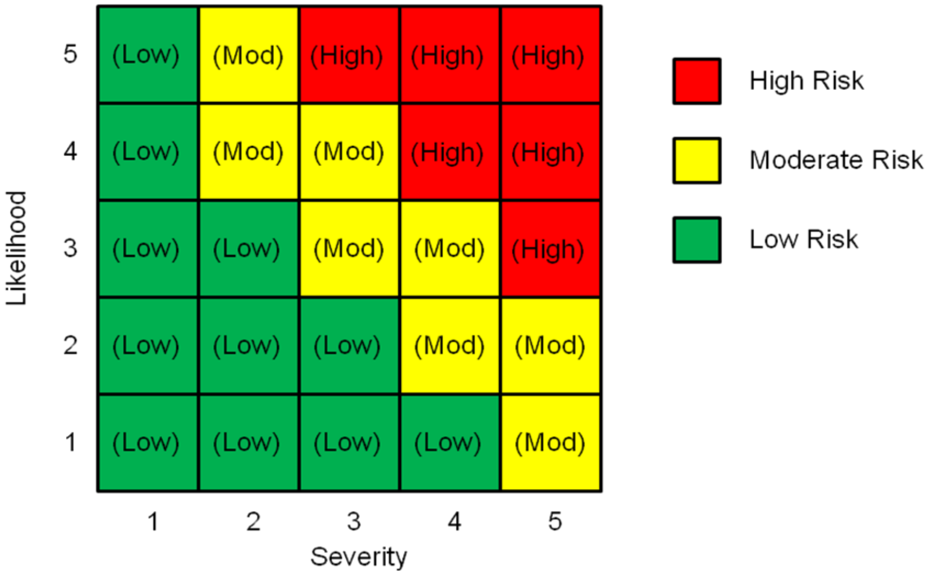
Using this document as a reference, the FMECA for SwampSat was performed. The severity of the effect on the system and the likelihood of the occurrence can be combined to provide a criticality number. The criticality number can be determined using the Risk Matrix [12], an example of which is shown in Figure 2-1. The definitions of each risk are [12, 16]:

- LOW RISK (Low). Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Actions within the scope of the planned program and normal management attention should result in controlling acceptable risk. Minimum impact. Criticality less than 6 except when likelihood is 1 and severity is 5.

- MODERATE RISK (Mod). May cause some increase in cost, disruption of schedule, or degradation or performance. Special action and management attention may be required to handle risk. Some impact. Criticality less than or equal to 8 and less than 15, except when likelihood is 1 and severity is 5.

- HIGH RISK (High). Likely to cause significant increase in cost, disruption of schedule, or degradation of performance. Significant additional action and high-priority management attention will be required to handle risk. Significant impact. Criticality greater than or equal to 15.

The criticality number is established based upon subjective and practical engineering judgment by the designers. Once the criticality of each failure mode is identified, the FMECA can be put in a tabular format in an orderly and organized manner. Since the individual failure modes are listed in a tabular format, the FMECA can be used to verify design integrity, identify and quantify sources of undesirable failure modes, and document the reliability risks. Different mitigation plans can be developed to reduce the possible failures in the SwampSat mission.



Likelihood	1	2	3	4	5
5	(Low)	(Mod)	(High)	(High)	(High)
4	(Low)	(Mod)	(Mod)	(High)	(High)
3	(Low)	(Low)	(Mod)	(Mod)	(High)
2	(Low)	(Low)	(Low)	(Mod)	(Mod)
1	(Low)	(Low)	(Low)	(Low)	(Mod)
	Severity				

🟥 High Risk

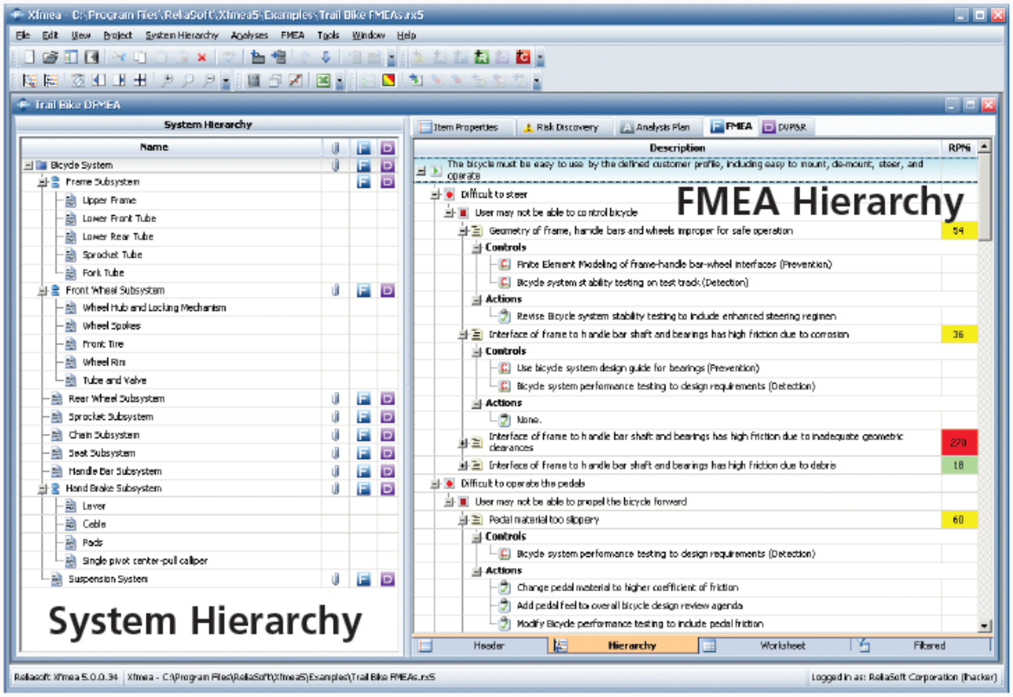
🟨 Moderate Risk

🟩 Low Risk

Figure 2-1. Risk matrix

Since the FMECA requires significant effort, designers and analysts have looked at alternative approaches to FMECA. Currently, a computer-based FMECA tool is widely common throughout the industries. Screen shot examples of the FMECA software from ReliaSoft, are shown in Figure 2-2 and Figure 2-3 [17]. Figure 2-2 shows the failures organized as a hierarchy which can be compressed or expanded accordingly. Figure 2-3 shows a worksheet which users can type directly in the cells for the analysis. The information can be entered in to the software and the program will summarize the worksheet data in a top-down report. Another approach to reduce the workload for the analysts is to perform the FMECA at the function level rather than by parts. If the failure modes for each of the functions can be defined, the designers and the analysts can perform the analysis with much less effort than from the parts list.

The computer-based FMECA software was not used for this thesis since it was beyond the cost of the project. Instead, the FMECA was developed using a Microsoft ® Excel worksheet.


Xfmea - C:\Program Files\ReliaSoft\Xfmea5\Examples\Trail Bike FMEAs.rx5
File Edit View Project System Hierarchy Analyses FMEA Tools Window Help
Trail Bike DFMEA
System Hierarchy
Item Properties
Risk Discovery
Analysis Plan
FMEA
DVP&R
Header
Hierarchy
Worksheet
Filtered

Name
Bicycle System
Frame Subsystem
Upper Frame
Lower Front Tube
Lower Rear Tube
Sprocket Tube
Fork Tube
Front Wheel Subsystem
Wheel Hub and Locking Mechanism
Wheel Spokes
Front Tire
Wheel Rim
Tube and Valve
Rear Wheel Subsystem
Sprocket Subsystem
Chain Subsystem
Seat Subsystem
Handle Bar Subsystem
Hand Brake Subsystem
Lever
Cable
Pads
Single pivot center-pull caliper
Suspension System

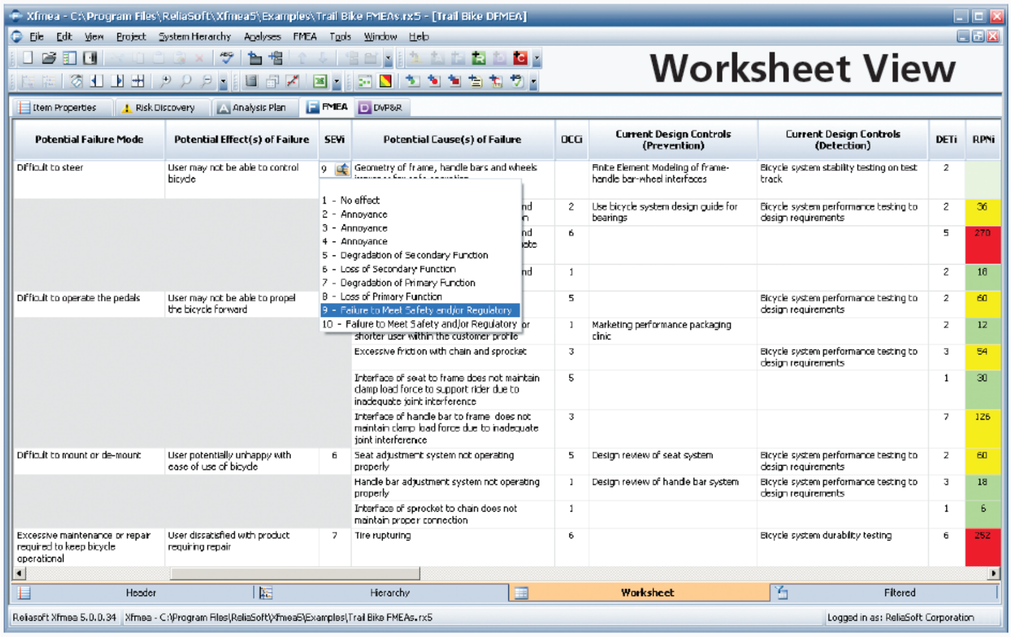
System Hierarchy

Description	RPNi
The bicycle must be easy to use by the defined customer profile, including easy to mount, de-mount, steer, and operate	
Difficult to steer	
User may not be able to control bicycle	
Geometry of frame, handle bars and wheels improper for safe operation	54
Controls	
Finite Element Modeling of frame-handle bar-wheel interfaces (Prevention)	
Bicycle system stability testing on test track (Detection)	
Actions	
Revise Bicycle system stability testing to include enhanced steering regimen	
Interface of frame to handle bar shaft and bearings has high friction due to corrosion	36
Controls	
Use bicycle system design guide for bearings (Prevention)	
Bicycle system performance testing to design requirements (Detection)	
Actions	
None.	
Interface of frame to handle bar shaft and bearings has high friction due to inadequate geometric clearances	270
Interface of frame to handle bar shaft and bearings has high friction due to debris	18
Difficult to operate the pedals	
User may not be able to propel the bicycle forward	
Pedal material too slippery	60
Controls	
Bicycle system performance testing to design requirements (Detection)	
Actions	
Change pedal material to higher coefficient of friction	
Add pedal feel to overall bicycle design review agenda	
Modify Bicycle performance testing to include pedal friction	

FMEA Hierarchy

Reliasoft Xfmea 5.0.0.34 | Xfmea - C:\Program Files\ReliaSoft\Xfmea5\Examples\Trail Bike FMEAs.rx5 | Logged in as: ReliaSoft Corporation (hacker)

Figure 2-2. Screen shot of FMECA software from ReliaSoft Inc.: hierarchy (Permission approved to use the image. Source: http://www.reliasoft.com/pubs/xfmea_brochure.pdf, last accessed June 10 2011)


Xfmea - C:\Program Files\ReliaSoft\Xfmea5\Examples\Trail Bike FMEAs.rx5 - [Trail Bike DFMEA]
File Edit View Project System Hierarchy Analyses FMEA Tools Window Help
Item Properties
Risk Discovery
Analysis Plan
FMEA
DVP&R
Header
Hierarchy
Worksheet
Filtered

Worksheet View

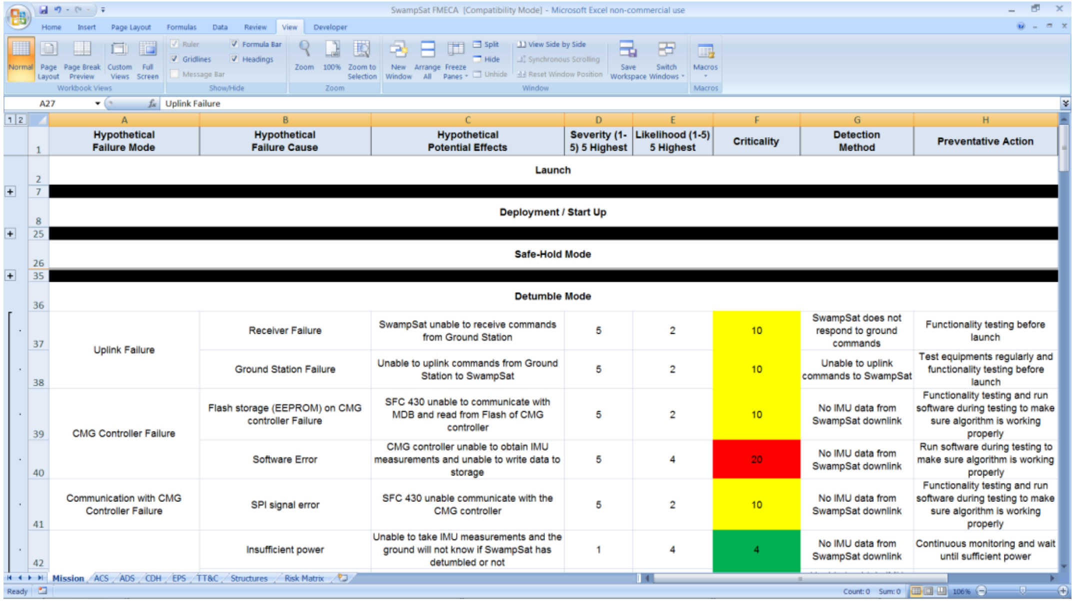
Potential Failure Mode	Potential Effect(s) of Failure	SEVi	Potential Cause(s) of Failure	OCCi	Current Design Controls (Prevention)	Current Design Controls (Detection)	DETi	RPNi
Difficult to steer	User may not be able to control bicycle	9	Geometry of frame, handle bars and wheels		Finite Element Modeling of frame-handle bar-wheel interfaces	Bicycle system stability testing on test track	2	
			nd n	2	Use bicycle system design guide for bearings	Bicycle system performance testing to design requirements	2	36
			nd ate	6			5	270
			nd	1			2	18
Difficult to operate the pedals	User may not be able to propel the bicycle forward			5		Bicycle system performance testing to design requirements	2	60
			or shorter user within the customer profile	1	Marketing performance packaging clinic		2	12
			Excessive friction with chain and sprocket	3		Bicycle system performance testing to design requirements	3	54
			Interface of seat to frame does not maintain clamp load force to support rider due to inadequate joint interference	5			1	30
			Interface of handle bar to frame does not maintain clamp load force due to inadequate joint interference	3			7	126
Difficult to mount or de-mount	User potentially unhappy with ease of use of bicycle	6	Seat adjustment system not operating properly	5	Design review of seat system	Bicycle system performance testing to design requirements	2	60
			Handle bar adjustment system not operating properly	1	Design review of handle bar system	Bicycle system performance testing to design requirements	3	18
			Interface of sprocket to chain does not maintain proper connection	1			1	6
Excessive maintenance or repair required to keep bicycle operational	User dissatisfied with product requiring repair	7	Tire rupturing	6		Bicycle system durability testing	6	252

1 - No effect
2 - Annoyance
3 - Annoyance
4 - Annoyance
5 - Degradation of Secondary Function
6 - Loss of Secondary Function
7 - Degradation of Primary Function
8 - Loss of Primary Function
9 - Failure to Meet Safety and/or Regulatory
10 - Failure to Meet Safety and/or Regulatory

Reliasoft Xfmea 5.0.0.34 | Xfmea - C:\Program Files\ReliaSoft\Xfmea5\Examples\Trail Bike FMEAs.rx5 | Logged in as: ReliaSoft Corporation

Figure 2-3. Screen shot of FMECA software from ReliaSoft Inc.: worksheet view (Permission approved to use the image. Source: http://www.reliasoft.com/pubs/xfmea_brochure.pdf, last accessed June 10 2011).

In the Excel ® worksheet, the following items were listed; the possible failure mode, possible cause of the failure, possible effects of the failure, severity and likelihood of the failure, criticality number, detection method, and preventative action. The Excel worksheet is explained in detail in the next chapter. The worksheet was programmed to calculate and change the color of the cell according to the criticality number. Figure 2-4 shows a screen shot example of the Excel ® worksheet used for this thesis. Similar to the computer-based FMECA software worksheet, the information was typed directly into the cells in the Excel worksheet. Also, the Excel worksheet was formatted to expand and collapse according to the failure stage.



	A	B	C	D	E	F	G	H
1	Hypothetical Failure Mode	Hypothetical Failure Cause	Hypothetical Potential Effects	Severity (1-5) 5 Highest	Likelihood (1-5) 5 Highest	Criticality	Detection Method	Preventative Action
2	Launch							
7								
8	Deployment / Start Up							
25								
26	Safe-Hold Mode							
35								
36	Detumble Mode							
37	Uplink Failure	Receiver Failure	SwampSat unable to receive commands from Ground Station	5	2	10	SwampSat does not respond to ground commands	Functionality testing before launch
38		Ground Station Failure	Unable to uplink commands from Ground Station to SwampSat	5	2	10	Unable to uplink commands to SwampSat	Test equipments regularly and functionality testing before launch
39	CMG Controller Failure	Flash storage (EEPROM) on CMG controller Failure	SFC 430 unable to communicate with MDB and read from Flash of CMG controller	5	2	10	No IMU data from SwampSat downlink	Functionality testing and run software during testing to make sure algorithm is working properly
40		Software Error	CMG controller unable to obtain IMU measurements and unable to write data to storage	5	4	20	No IMU data from SwampSat downlink	Run software during testing to make sure algorithm is working properly
41	Communication with CMG Controller Failure	SPI signal error	SFC 430 unable communicate with the CMG controller	5	2	10	No IMU data from SwampSat downlink	Functionality testing and run software during testing to make sure algorithm is working properly
42		Insufficient power	Unable to take IMU measurements and the ground will not know if SwampSat has detumbled or not	1	4	4	No IMU data from SwampSat downlink	Continuous monitoring and wait until sufficient power

Figure 2-4. Screen shot of Excel ® worksheet

2.3 Introduction to FTA

FTA is an alternative analytical technique which complements FMECA by starting with a top-level failure effect and tracing the failure to potential causes. Typically, the analysis begins with an existing FMECA. FMECA includes all parts or function of a system, whereas FTA is applied selectively to the most severe failure effects. Using the most severe failure effects from the FMECA, a fault tree can be constructed. The fault tree evaluates the combinations of failures that can lead to the top event of interest [12, 18, 19]. The fault tree is constructed using the FTA symbols, also known as logic gates, to represent events and consequences and describe the logical relationship between events. The FTA symbols are shown in Figure 2-5. The event is represented by a rectangle and it can result from a combination of singular events. The top-level failure is represented by the rectangle. Once the top-level failure has been selected, the analyst needs to identify the immediate causes. The causes can be either additive (either cause A or cause B will result in the top event) or complementary (both must occur to cause the top event). The additive causes and the complementary causes are represented by an OR-gate and an AND-gate, respectively [10]. The continuation symbol can be used to show an extension of a complex fault tree which is represented by a triangle. Once the failure cannot be expanded further, then a basic failure symbol, represented by a circle, can be used. Once the basic failure events have been identified, the critical components and the critical paths can be further evaluated [20, 21].

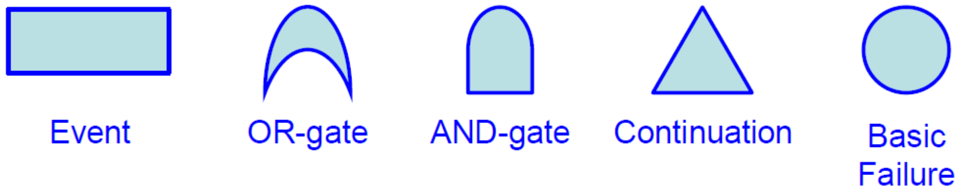
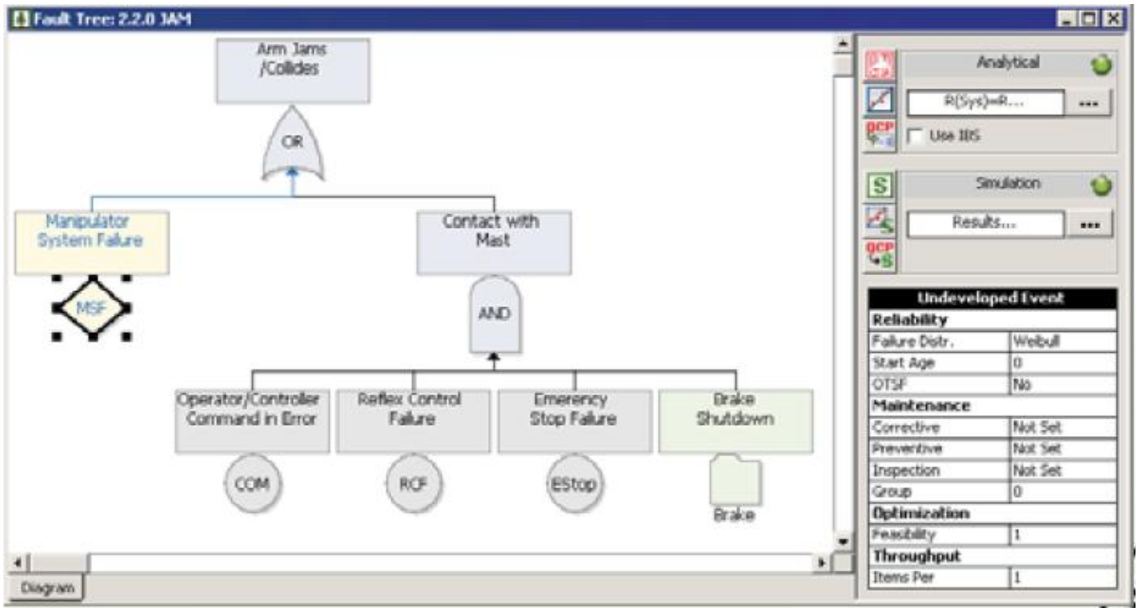


Figure 2-5. FTA symbols

Similar to the FMECA, the FTA is commonly constructed using computer-based software. However, the FTA for this thesis was constructed using Microsoft ® Power Point due to the high cost of the software. The top failure event for the SwampSat FTA was the SwampSat mission failure and by using the logic gates, the top failure event was divided into lower level failures. The software uses a simple drag-and-drop technique to build the FTA. However in the Power Point ®, each symbols had to be generated and modified to appropriate sizes as shown in Figure 2-5. Figure 2-6 shows a screen shot example of the FTA from ReliaSoft [22] and using this as a reference, the SwampSat FTA was constructed. The SwampSat FTA is given in detail in Chapter 4. As one can see in Figure 2-6, the top level event can be expanded out using the logic gates to identify the basic level failures.



R(Sys)=R...

□ Use IBS

Results...

Undeveloped Event	
Reliability	
Failure Distr.	Weibull
Start Age	0
OTSF	No
Maintenance	
Corrective	Not Set
Preventive	Not Set
Inspection	Not Set
Group	0
Optimization	
Feasibility	1
Throughput	
Items Per	1

Figure 2-6. Screen Shot of FTA software from ReliaSoft Inc. (Permission approved to use the image. Source: http://www.reliasoft.com/pubs/blocksim_brochure.pdf, last accessed June 10 2011).

CHAPTER 3
SWAMPSAT FMECA

3.1 Introduction to SwampSat FMECA

As stated earlier, SwampSat is the first CubeSat being designed and developed by the University of Florida. Failure, Modes, Effects, and Criticality Analysis (FMECA) is one of the analyses used to investigate how or where SwampSat might fail. For the SwampSat FMECA, the Microsoft ® Excel worksheet was used. As mentioned previously, the cost of the software was too expensive for this effort, therefore, the Microsoft ® Excel worksheet was used. The worksheet included the following columns:

- Hypothetical Failure Mode
- Hypothetical Failure Cause
- Hypothetical Potential Effects
- Severity (1 - 5)
- Likelihood (1 - 5)
- Criticality (product of severity and likelihood)
- Detection Method
- Preventative Action

The first column labeled “Hypothetical Failure Mode” lists a single part or an operational mode in which the failure could occur. The column labeled “Hypothetical Failure Cause” lists the reason why a particular failure mode could occur. The cause of a certain failure could be due to a single failure or multiple of other lower level failures. The third column, “Hypothetical Potential Effects” lists the consequences that arise due to the particular failure mode. Not only could a single consequence occur, but multiple consequences could transpire as well. The next two columns, “Severity” and “Likelihood”, are used for the criticality analysis. Both severity and likelihood rankings are listed in numbers ranging from 1 to 5 with 5 being the highest level. The level of severity and likelihood are shown in Table 3-1 and Table 3-2, respectively [16].

Table 3-1. Level of severity (LS) of failure

Level	Severity of the Failure
1	Minimal or No Impact
2	Acceptable with Some Reduction in Margin, Some Impact
3	Acceptable with Significant Reduction in Margin, Moderate Impact
4	Acceptable, No Remaining Margin, Major Impact
5	Unacceptable

Table 3-2. Level of likelihood (LL) of occurrence

Level	Likelihood of Occurrence
1	Remote; Components with Rich Space Heritage
2	Unlikely; COTS and Components with Space Heritage
3	Likely; COTS and Built in-house Components with Some Space Heritage
4	High Likely; Built in-house Components with No Space Heritage
5	Near Certainty; Built in-house Components with No Space Heritage

The severity ranking is based on the SwampSat mission failure where the most severe level LS5 refers to complete SwampSat mission failure. The likelihood of occurrence was ranked based on space heritage and commercial off-the-shelf (COTS) components. The level LL1 is assigned to components with rich space heritage and high successes in the past and has a remote likelihood of failure occurrence. The level LL2 is assigned to COTS components and components with some space heritage and failure is unlikely to occur. The level LL3 is assigned to COTS and in-house built components with some space heritage and failure is likely to occur. Levels LL4 and the LL5 are both ranked for built in-house components with no space heritage. The only difference between the two levels is that the Technology Readiness Level (TRL) [23] of LL4 components is higher than that of LL5 components. For example, LL5 rankings are given to items such as the CMGs and the Sun sensors, since both are built in-house for the first time and they are both at TRL 4. Software algorithm errors are given LL4 ranking since the programming is done in-house and the TRL is at 6.

As mentioned earlier, using the risk matrix, the criticality number was computed by multiplying the number from the “Severity” column by the number from “Likelihood” column. The criticality number was then listed in the column labeled “Criticality”. The Excel ® worksheet was programmed to change the color according to the criticality number to represent the risk. The next column labeled “Detection Method” lists how the failure mode could be identified. The failures should be detected at the lowest possible level so that the failed component can be identified and necessary actions could be taken. The last column, “Preventative Action” lists the ways the failure mode can be eliminated or reduced. The verification matrix for SwampSat [24] shows four different methods of testing for SwampSat, test and measurement, analysis and simulation, observation and inspection, and reference and datasheet. Using one or more methods from the verification matrix, the “Preventative Action” column was developed.

For the SwampSat mission FMECA, the mission profile was divided into seven different stages:

- Launch
- Deployment/Start Up
- Safe-Hold Mode
- Detumble Mode
- Comms Mode
- ADS Mode
- CMG Ops Mode

The launch stage was added in the analysis to understand the importance of the launch. This is based on an examination of past CubeSat missions where the main reason that the CubeSats failed were due to launch failure. Table 3-3 shows the past CubeSats failures [25]. To ensure success of the launch vehicles, the Federal Aviation

Administration (FAA) developed a safety guide for reusable launch and reentry vehicles [26].

Table 3-3. Past CubeSat failures

Name of CubeSat	Launch Date	Reasons of Failure
CanX-1	6/30/2003	No Communication after Launch
DTUsat-1	6/30/2003	No Communication after Launch
AAU CubeSat	6/30/2003	Weak Signal after Launch; Battery Failure
NCUBE-2	10/27/2005	No Communication after Launch
UWE-1	10/27/2005	Contact Lost
SACRED	7/26/2006	Launch Failure
ION	7/26/2006	Launch Failure
Rincon 1	7/26/2006	Launch Failure
ICE Cube 1	7/26/2006	Launch Failure
KUTESat	7/26/2006	Launch Failure
NCUBE-1	7/26/2006	Launch Failure
HAUSAT-1	7/26/2006	Launch Failure
SEEDS-1	7/26/2006	Launch Failure
CP-2	7/26/2006	Launch Failure
Aero Cube 1	7/26/2006	Launch Failure
MEROPE	7/26/2006	Launch Failure
Mea Huaka'I (Voyager)	7/26/2006	Launch Failure
ICE Cube 2	7/26/2006	Launch Failure
CP-1	7/26/2006	Launch Failure
PicPot	7/26/2006	Launch Failure
AeroCube 2	4/17/2007	Solar Converter Malfunction
PREsat	8/3/2008	Launch Failure
NanoSail-D	8/3/2008	Launch Failure
Hayato	5/20/2010	No Communication after Launch
KySat-1	3/4/2011	Launch Failure
Hermes	3/4/2011	Launch Failure
Explorer-1'	3/4/2011	Launch Failure

Note: Table obtained by AMSAT website (http://www.amsat.org/amsat-new/satellites/history.php, last accessed Sept. 3 2010)

3.2 Launch

The launch stage includes before and during launch period of the mission. The FMECA of the launch stage is shown in Table 3-4. The FMECA for the SwampSat mission began by assuming that SwampSat met all the criteria before launch. Some of the standards that SwampSat needs to meet are CubeSat Design Specification (CDS) document [4], 1U CubeSat Acceptance Checklist (CAC) [27], P-POD Interface Control Document (ICD) [28], and also mission requirements by the launch provider [29]. Once all the criteria are met, SwampSat will be placed inside a P-POD or another orbit deployer. Assuming a P-POD deployment, once SwampSat is placed inside the P-POD, its remove before flight (RBF) pin will be removed. The RBF pin is required to keep the CubeSats inactive during the final integration into the P-POD [4]. While the RBF pin is intact, the Electrical Power System (EPS) for SwampSat will not be activated and if the RBF pin removal fails due to mechanism issues, SwampSat will not be powered up. The RBF pin is built in-house using the CDS document, therefore, the likelihood of failure was listed as likely (LL3). If the RBF pin is not able to be removed, SwampSat will have to be taken out from the P-POD, thus, the severity was listed as moderate impact (LS3). The RBF pin failure can be detected while SwampSat is still on the ground and by performing functionality tests, observation, and inspection before launch, the RBF pin failure can be prevented. Once the RBF pins are removed, the P-PODs will be loaded on to the launch vehicle and SwampSat will await launch.

During launch, both the launch vehicle and the P-POD could fail. The launch vehicle could fail from acoustic shocks, vibrations or from other catastrophic failure. Obviously if the launch vehicle fails, then SwampSat along with other CubeSats and the primary payload will never reach orbit, so the severity was ranked as unacceptable (LS5). Past experience has shown that it is unlikely that the launch vehicle will fail during launch, but as mentioned earlier, most of the past CubeSat failures were due to launch failure, therefore, the likelihood of the launch vehicle failure was ranked as unlikely (LL2). If the launch vehicle fails during launch, the launch service provider

(LSP) will communicate the message to all the CubeSat developers. The only way the launch vehicle failure can be prevented will be tests done by the LSP. Not only could the launch vehicle fail during launch, the P-POD could also fail from shock and vibration. P-POD failure results in SwampSat and other CubeSats mission failure, therefore, the severity was ranked as unacceptable (LS5). However, there has been no record of P-POD failures in the past, therefore, the likelihood of the P-PODs failing was listed as remote (LL1). The P-POD failure can only be detected after launch and the only way to avoid the failure will be to perform proper tests conducted by Cal Poly.

Table 3-4. Launch stage FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
RBF pin failure	RBF removal mechanism failure	Unable to power up EPS	3	3	9 (Mod)	Able to detect failure before launch	Functionality testing, observe and inspect before launch
Launch vehicle failure	Breaks due to shocks and vibrations	Launch vehicle, P-Pod and SwampSat mission will fail.	5	2	10 (Mod)	Launch fail confirmation from the LSP	Test done by LSP
Launch vehicle failure	Launch vehicle burns up	Launch vehicle, P-Pod and SwampSat mission will fail	5	2	10 (Mod)	Launch fail confirmation from the LSP	Test done by LSP
P-POD failure	Breaks due to shocks and vibrations	SwampSat will not be deployed and mission will be a failure	5	1	5 (Mod)	No communication from any CubeSats. Can only be detected after launch	Proper test by Cal Poly

Although no high criticality failures were identified in the launch stage, moderate criticality items were identified. As previously mentioned, the launch vehicle and the P-

POD are the responsibility of Cal Poly and the LSP, therefore, the SwampSat team will have no control. On the other hand, the SwampSat team must take a closer look at design and development of the RBF pin.

3.3 Deployment / Startup

The FMECA for the deployment/start up stage is shown in Table 3-5 and the software architecture [7] is shown in Appendix A-1. After successful launch, SwampSat and the other CubeSats will be deployed into orbit. Once in orbit, SwampSat and other CubeSats will be deployed out from the P-POD [1, 29].

Table 3-5. Deployment/Startup stage FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Deployment failure from P-POD	P-POD door does not open correctly to deploy CubeSats in to orbit	SwampSat and other CubeSats will not be deployed	5	1	5 (Low)	No communication from any CubeSats	Proper test by Cal Poly
	Deployment spring mechanism failure	SwampSat and other CubeSats will not be deployed	5	1	5 (Low)	No communication from any CubeSats	Proper test by Cal Poly
	Premature antenna deployment	SwampSat and other CubeSats will not be deployed. Antenna system could be damaged	5	3	15 (High)	No communication from any CubeSats. Weak signals from SwampSat	Vibration testing on antenna deployment system
Start Up failure; EPS and CDH do not power up	Dead batteries	Unable to start up EPS and CDH. Unable to recharge the batteries	5	2	10 (Mod)	No communication from SwampSat	Functionality testing

Table 3-5. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Start Up failure; EPS and CDH do not power up	Deployment switch malfunction	Unable to start up EPS and CDH	5	2	10 (Mod)	No communication from SwampSat	Functionality testing, observation, and inspection
	Separation spring failure	Unable to separate from other CubeSats; Unable to activate deployment switch	3	2	6 (Low)	Weak signal received from SwampSat	Observation and inspection
	CDH failure	Unable to operate SwampSat	5	3	15 (High)	No communication from SwampSat	Functionality testing, analysis and simulation
	EPS failure	Unable to provide power for SwampSat	5	2	10 (Mod)	No communication from SwampSat	Functionality testing, observation, and inspection
Data failure	RTC failure	Unable to provide real-time	3	2	6 (Low)	No real-time data in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
	EEPROM on SFC430 failure	Unable to store data	5	2	10 (Mod)	No data from SwampSat downlink	Functionality testing and run software during testing
Antenna deployment failure	Insufficient power	Unable to burn the nichrome filament and antennas will not be deployed	1	4	4 (Low)	Launch lag =0. Weak signal received from SwampSat	Continuous monitoring and wait until sufficient power

Table 3-5. Continued.

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Antenna deployment failure	Antennas do not fully deploy due to burn wire mechanism	Antennas can be used for communication to the ground station, however, the signals will be very weak	5	3	15 (High)	Launch Flag =0. Weak signal received from SwampSat	Functionality testing, observation , and inspection
	Antenna system failure	Unable to use antennas for communication	5	3	15 (High)	No communication with SwampSat	Functionality testing, observation , and inspection
	Load switch malfunction	SFC430 unable to turn load switch on to burn the nichrome filament	5	2	10 (Mod)	Launch Flag =0 from SwampSat downlink	Functionality testing
Connection failure	Cabling failure	No connection and communication between interfaces	5	3	15 (High)	No communication with SwampSat	Ground testing before launch for proper connection between interfaces
Software error in algorithm	Programming error	Unable to read real-time, store boot counter, store boot time, deploy antenna, and read and store launch flag	5	4	20 (High)	No communication with SwampSat	Run software during testing to ensure algorithm is working

Deployment failure from the P-POD could occur from P-POD door not opening properly, deployment spring mechanism failure, and premature antenna deployment. In order for SwampSat and other CubeSats to deploy from the P-POD, the door of the P-POD must open. If the P-POD door does not open, SwampSat and the other CubeSats will not be ejected out from the P-POD and this will result in the mission failure, thus, the severity was ranked at unacceptable (LS5). Once the P-POD door is opened, the deployment spring mechanism will eject SwampSat and other CubeSats out from the P-POD. If the deployment spring mechanism fails, SwampSat and the other CubeSats will not be deployed out from the P-POD, so the severity was ranked as unacceptable (LS5). Cal Poly has performed numerous tests to ensure that the P-POD door mechanism and the deployment spring mechanism function properly, therefore, the likelihood that the mechanisms could fail was decided as remote (LL1) [2, 29]. While inside the P-POD, SwampSat antenna mechanism could prematurely deploy from shocks and vibrations, causing SwampSat to be stuck inside the P-POD. If SwampSat does get ejected out from the P-POD with the antennas pre-deployed, the antenna system will be damaged and could result in a poor or no communication and may end SwampSat's mission, therefore, the severity was ranked as unacceptable (LS5). Since the antenna system and the antenna deployment mechanism are built in-house, the likelihood was ranked as likely (LL3). The deployment failure from the P-POD can only be detected after launch. The P-POD door mechanism and the P-POD deployment spring mechanism are both developed and tested by Cal Poly to prevent any failures. In order to avoid the SwampSat antenna system from prematurely deploying, the antenna system will be put through multiple vibration tests to ensure there is no antenna deployment while in the P-POD.

After deployment from the P-POD, the separation springs will provide relative separation between SwampSat and other CubeSats and the deployment switches will be activated. The deployment switches are deactivated during integration in order to keep the CubeSats' power completely turned off during launch. After the deployment switches are deactivated, the SwampSat Electrical Power System (EPS) and the flight computer, SwampSat Flight Computer (SFC430), will be powered on. SFC430 is the SwampSat main flight computer with a MSP 430 based microcontroller [30]. Startup failure could occur from malfunctions of separation spring, deployment switch, battery, EPS, and Command and Data Handling (CDH). The separation spring malfunction could cause SwampSat not to separate from other CubeSats, therefore, the severity was listed as moderate impact (LS3). The separation spring is a commercial off-the-shelf (COTS) component as listed in the CDS [4], thus, the likelihood was listed as unlikely (LL2). If the springs do fail, SwampSat might not have enough separation and could interfere with other CubeSats. Furthermore, the ground station could get weak or no signals from SwampSat due to the interferences from the other CubeSats. The malfunction of the deployment switches will be more severe. If the deployment switches remain activated, SwampSat EPS and CDH will never be powered up and SwampSat will not be able to complete the mission, so the severity was ranked as unacceptable (LS5). The deployment switch is a COTS component, therefore, the likelihood was listed as likely (LL2). If the switch malfunctions, the SwampSat EPS subsystem and the SFC430 will not be powered up and the ground station will receive no communication from SwampSat. The separation spring will be tested by observation and inspection to ensure the spring works properly. To avoid the deployment switch failure, functionality test as well as observation and inspection will be conducted before launch.

Following the deployment switch activation, the battery on the EPS board can be charged. If for any reason the battery is unable to charge, the SwampSat mission will result in a failure. The SwampSat EPS subsystem can also fail to provide power for SwampSat. If the EPS subsystem fails, the SwampSat mission will also be a failure. For both failures, the severity was ranked as unacceptable (LS5). However, the battery and the components on the EPS board are COTS components from Clyde Space, who has experience with high performance power systems for small satellites [31], therefore, the likelihood of occurrence was listed as unlikely (LL2). FMECA for the SwampSat EPS subsystem is shown in Appendix B-4. Also, the SwampSat mission would not be a success without the CDH subsystem. The CDH subsystem contains the SFC430, the main flight computer for SwampSat and if the SFC430 fails, SwampSat will not be able to execute any tasks, therefore, the severity was ranked as unacceptable (LS5). The SFC430 is custom built in-house for SwampSat mission, thus, the likelihood of CDH failing was ranked as likely (LL3). Detailed FMECA of the SwampSat CDH subsystem are listed in Appendix B-3. When the EPS or the CDH subsystems fail, there will be no communication between the ground station and SwampSat. For the EPS subsystem, functionality tests, observations, and inspections will be performed during testing. Functionality tests, analyses, and simulations on the mission operations software will be performed to ensure the CDH subsystem can execute appropriately.

After the EPS and the SFC430 have been powered up, SFC430 will read the time from the real-time clock (RTC) via Inter-Integrated Circuit (I2C) and write the data to the Electrically Erasable and Programmable Read Only Memory (EEPROM) on the SFC430 board, also known as the flash storage, also via I2C. The real-time will be recorded as boot time and the boot count will be updated on the EEPROM. The boot count is the number of times SwampSat reboots during the mission. For the SwampSat mission FMECA, the RTC and the EEPROM failures are noted as data failure. If RTC fails, SFC430 will not be able to read the time from the RTC. RTC failure does not necessarily cause the SwampSat mission to fail, however, the failure will cause a moderate effect on the SwampSat mission, thus, severity was ranked as moderate impact (LS3). Executions of each operation depend on time, so by not knowing the real-time, the executions will be very difficult. If the EEPROM on the SFC430 fails, no data can be stored nor read by the SFC430. EEPROM failure was ranked as unacceptable (LS5) since data storage is needed for the SwampSat mission. One of the SwampSat mission requirements is to transmit the stored data to the ground station and if the EEPROM cannot store data, the SwampSat mission will be over. Both the RTC and the EEPROM on the SFC430 are COTS components, therefore, the likelihood of these components failing was ranked as unlikely (LL2). Further analyses of these two components can be seen in the FMECA of CDH subsystem in Appendix B-3. In order to prevent the data failure, both the RTC and the EEPROM will be tested by running the software to check the algorithms are working accordingly.

The SFC430 will read the launch flag from the EEPROM on the SFC430 to determine if the deployment and the wait period have been successfully executed. Initially the launch flag is set at 0 so the antennas can be deployed and once the antennas have been deployed, the launch flag will be set to 1. CubeSats must wait at least a minimum of 30 minutes to deploy the antennas after the deployment switches are deactivated, but for additional safety SwampSat is designed to wait 45 minutes. The wait period ensures no interference with the primary payload and is a mandatory procedure [3]. Following the wait period, both receive and transmit antennas will be deployed. Antenna deployment is one of the major factors of the SwampSat mission [32]. If the antenna deployment fails, ground station will not be able to receive and send telemetry to SwampSat. Antenna deployment may fail due to insufficient power, burn wire mechanism, antenna system failure, and the load switch malfunction. Insufficient power to burn the nichrome filament, the burn wire, is not a major issue. SwampSat can wait until sufficient power to burn the filament again when there is insufficient power. Insufficient power could occur frequently, so the likelihood was listed as highly likely (LL4). The batteries can be recharged and the antenna deployment could be attempted again, therefore, the severity was listed as no impact (LS1). If the burn wire mechanism fails, the antenna will not be fully deployed and the signals received from SwampSat will be very weak. Also, the commands sent from the ground station might not be picked up by SwampSat if the antennas are not fully deployed, therefore, the severity was listed as unacceptable (LS5). If the antenna system fails, there will be no communication with SwampSat, so severity was ranked as unacceptable (LS5). The antenna system can be divided into a receive antenna module and a transmit antenna module. Receive antenna module failure results in SwampSat not being able to receive commands from the ground station. Transmit antenna module failure results in no telemetry downlink from SwampSat. FMECA of the antenna system can be seen in the Telemetry, Tracking and Command (TT&C) subsystem FMECA in Appendix B-5. The burn wire mechanism and the antenna systems are both built in-house, therefore, for both the likelihood of the failures was ranked as likely (LL3). If the launch flag remains at 0 and the ground station is receiving weak signals from SwampSat, either insufficient power or the burn wire mechanism failure occurred. Another antenna deployment failure could be caused from malfunction of the load switch. Activation of the load switch allows the current to pass through to burn the nichrome filament for antenna deployment. If the load switch malfunctions, the current will not pass through and the antennas will not be deployed. The load switch failure could cause SwampSat mission to be a failure due to lack of communication between SwampSat and the ground station, thus, severity was ranked as unacceptable (LS5). However, the load switch is a COTS item so the likelihood of the load switch to malfunction was listed as unlikely (LL2). To avoid antenna deployment failure, functionality tests will be performed for the burn wire mechanism, antenna system, and the load switch. Observations and inspections for any problems would be necessary while testing the burn wire mechanism and the antenna system.

As in the software architecture, the launch flag status is updated once the load switch has been activated. The acceleration readings from the Inertial Measuring Unit (IMU) are taken before and after the activation of the load switch and if the difference between the two readings are greater than a predefined threshold, the launch flag status will be set at 1 and if there are no difference, the launch flag status will remain 0. The ground station can command SwampSat to redeploy the antennas if necessary.

During the deployment/startup stage, if there are any connection failures between interfaces or any software errors the SwampSat mission will be a failure, thus, the severity was ranked as unacceptable (LS5). The connection failure could occur from cabling failure. All the cabling is done in-house, therefore, the likelihood of the connection failure occurring was ranked as likely (LL3). The software algorithm to perform the deployment/startup operation could fail due to programming error. The likelihood of the software error occurring was listed as highly likely (LL4) since all the software is designed and developed in-house. When there are no communications with SwampSat, these two failures could have occurred. To prevent the connection failure from happening, proper connection testing between interfaces must be performed before launch. Also, the software will be tested by running simulations to ensure the algorithm is working properly.

For the deployment/startup stage, several high criticality items were discovered. Several antenna related failures were identified as high criticality. Premature antenna deployment while SwampSat is still inside the P-POD will possibly lead to the SwampSat mission failure. The antenna deployment failure due to burn wire mechanism will result in SwampSat mission failure as well. Another antenna failure is the antenna system failure. With the antenna system failure, communication links in both directions will not be established. For all these possible failures, well thought plans must be created for functionality tests. Another high criticality item is the deployment switch. The switch must be tested for its functionality numerous times to ensure the switch will function. CDH subsystem is also a high criticality item. The SFC430 is the main flight computer for SwampSat and it is also the main component in the CDH subsystem. Since the SFC430 is custom built in-house, everything on the SFC430 must be checked carefully for its functionality. Another key part in the CDH subsystem is the software for SwampSat. Careful debugging and simulations must be conducted to avoid any software errors. The cabling is the last high criticality item listed. Each connection must be tested during integration and different methods of securing the cabling must be thought out. One possible method might be to apply a layer of epoxy on the connections to prevent them from coming loose.

Not only should there be special attention paid to the high criticality items, both the moderate and low risk items must be carefully examined also. Proper functionality tests must be performed on the hardware and a thorough debugging must be done on the software.

3.4 Safe-Hold

Once the deployment/startup stage is completed, SwampSat will enter the main operating mode known as the safe-hold mode. SwampSat is designed to operate mainly in the safe-hold mode to charge the on-board batteries in order to perform other operations. During the safe-hold mode, the SwampSat transceiver will be turned on to transmit and receive data to and from the ground station. While the receiver listens for ground commands, the transmitter can communicate the real-time satellite health data in specific intervals to the ground station. The ground station can command SwampSat to enter different operating modes according to the health data. The real time safe-hold mode downlink is also known as the SwampSat beacon and the downlink telemetry for the safe-hold mode is shown in Appendix C-1. The software architecture for the safe-hold mode can be seen in Appendix A-1.

The safe-hold FMECA is listed in Table 3-6. The first failure mode listed is the uplink failure. The uplink failure can be caused by either the receiver failure or the ground station failure. When the SwampSat receiver fails, the commands sent from the ground station will never be picked up by SwampSat, so the severity was ranked as unacceptable (LS5). Ground station failure will mean no commands will be sent to SwampSat, thus, severity was ranked as unacceptable (LS5). For both failures, SwampSat will remain in the safe-hold mode since there will be no commands to order SwampSat to enter a different operating mode. In safe-hold downlink, known as SwampSat beacon, failure mode can be caused by the transmitter failure, ground station failure, or query beacon failure. Query beacon is a function in the program where

SwampSat will gather health data from the control moment gyroscope (CMG) controller, Electrical Power System (EPS) board, transceiver board, real-time clock (RTC), electrically erasable programmable read-only memory (EEPROM), and the temperature sensors. The communications between the interfaces are executed using Inter-Integrated Circuit (I2C) or Serial Peripheral Interface (SPI). Transmitter failure will result in no downlink telemetry and no communication from SwampSat, therefore, the severity was ranked as unacceptable (LS5). Ground station failure will lead to no commands uplinked to SwampSat, so severity was ranked as unacceptable (LS5). The function query beacon failure will result in no health data obtained from SwampSat. Not knowing the health of SwampSat will not necessary result in mission failure, however, the ground station will not be able to make decisions for SwampSat to enter another operating mode, therefore, the severity was ranked as major impact (LS4). The transceiver board has commercial off-the-shelf (COTS) components which house both the receiver and the transmitter, therefore the likelihood of failure was ranked as unlikely (LL2). The equipment in the ground station is well monitored and the likelihood that the equipment will fail was listed as remote (LL1). Detailed FMECA of the SwampSat transceiver board and the ground station equipment are in Telemetry, Tracking & Command (TT&C) subsystem FMECA, located in Appendix B-5 and the FMECA for function query beacon is in Appendix B-3, Command and Data Handling (CDH) subsystem FMECA. The transceiver would be put through functionality testing to validate the communication. The ground station equipment will also be tested for their functionality to avoid any failures. To prevent any failures for the function query beacon, the algorithm would be tested and debugged.

Table 3-6. Safe-Hold mode FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Uplink failure	Receiver failure	SwampSat unable to receive commands from ground station	5	2	10 (Mod)	SwampSat does not respond to ground commands	Functionality testing
	Ground station failure	Unable to uplink commands from ground station to SwampSat	5	1	5 (Low)	Unable to uplink commands to SwampSat	Test equipment regularly and functionality testing
Downlink (SwampSat beacon) failure	Transmitter failure	SwampSat unable to transmit Safe-Hold mode downlink telemetry to ground station	5	2	10 (Mod)	No satellite health data from SwampSat	Functionality testing
	Query beacon failure	Unable to read telemetry from CMG Controller, EPS board, Transceiver, RTC, Flash, and temperature sensor	4	4	16 (High)	No satellite health data from SwampSat	Run software during testing to ensure algorithm is working
	Ground station failure	Unable to receive telemetry from SwampSat	5	1	5 (Low)	Unable to receive telemetry from SwampSat	Test equipment regularly and functionality testing
Battery charge failure	EPS failure	Unable to charge and store power to operate other modes	5	2	10 (Mod)	No power information from SwampSat downlink	Functionality testing, observation, and inspection before launch

Table 3-6. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Connection failure	Cabling failure	No connection and communication between interfaces	5	3	15 (High)	No communication with SwampSat	Ground testing before launch for proper connection between interfaces
Software error in Safe-Hold algorithm	Programming error	Unable to operate Safe-Hold mode	5	4	20 (High)	No communication with SwampSat	Run software during testing to ensure algorithm is working

As mentioned earlier, the safe-hold mode is designed to store power in order to perform other operations. If the batteries are unable to store power, SwampSat will not be able to execute different operations to complete the mission. For that reason the severity of the battery charge failure was ranked as unacceptable (LS5). The battery charge failure could be caused by the EPS failure. The EPS failure is fatal to the SwampSat mission, so the severity was ranked as unacceptable (LS5). Though the severity was ranked the highest, the EPS consists of COTS components, therefore, the likelihood of the failure was ranked as unlikely (LL2). Again, the FMECA for the EPS subsystem can be seen in Appendix B-4. To prevent any failures caused by environmental conditions, the components on the EPS board including the battery will go through functionality testing and also environmental testing in the thermal vacuum chamber and on the vibration shaker table.

The connection failure and the software algorithm error for the safe-hold mode could occur also. Since the safe-hold operating mode is the main operating mode for the SwampSat mission, the software error for the safe-hold mode would be a costly failure, thus, the severity was ranked as unacceptable (LS5). With no connection between the interfaces, SwampSat mission will be failure as well, so the severity was ranked as unacceptable (LS5). The likelihood for the connection failure was ranked as likely (LL3) and highly likely (LL4) for the software error.

Looking at Table 3-6, the high criticality items are the query beacon and safe-hold mode algorithms and the cabling error. Careful debugging of the software will be important not only for the safe-hold mode, but for all the other modes as well. As mentioned earlier, a well planned test procedure must be developed to check the connections on SwampSat.

3.5 Detumble Mode

Once SwampSat stores enough power during the safe-hold operating mode, the ground station will send commands to SwampSat to perform attitude maneuvers. However, when SwampSat and the other CubeSats are ejected out from the P-POD, the satellites are ejected out with a nominal rate of about 2 m/s. The ejection rate will be modified to meet the launch vehicle requirements [1, 29]. Before any attitude maneuvers can be performed, SwampSat must be stabilized. The detumble operating mode is designed to stabilize SwampSat about its three axes in order to perform the attitude maneuvers. Also, the detumble operating mode is designed as a timed operation where the ground station will command the specific time period. The software architecture for the detumble mode can be seen in Appendix A-3 and the detumble downlink telemetry data is shown in Appendix C-2.

The FMECA for the detumble mode is shown in Table 3-7. As mentioned earlier, the main goal of this operating mode is to stabilize the angular rates of the satellite. In order to check the angular rates, the SFC430 will query the CMG controller for the inertial measuring unit (IMU) rates and compare them to predefined reference rates. The CMG controller is a high performance digital signal processor (DSP) from Texas Instruments (TI) Inc and is referred to as the TI-DSP [33]. The communication between the SFC430 and the CMG controller is done through serial peripheral interface (SPI) link. If there are differences between the measured angular rates and the predefined angular rates, the SFC430 will command power to the magnetic coils. When the current runs through the magnetic coils, a magnetic field is generated. The magnetic field from the magnetic coils will interact with the Earth's magnetic field to stabilize the satellite. The magnetic coils are embedded on the SwampSat's printed circuit board (PCB) solar panels located on five sides of the satellite.

SwampSat will not enter the detumble operating mode if it does not receive commands from the ground station. As before, the uplink failure could occur from the failures of the SwampSat receiver or of the ground station.

Table 3-7. Detumble mode FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Uplink failure	Receiver failure	SwampSat unable to receive commands	5	2	10 (Mod)	SwampSat does not respond to ground command	Functionality testing
	Ground station failure	Unable to uplink commands from ground station to SwampSat	5	1	5 (Low)	Unable to uplink command to SwampSat	Test equipment regularly and functionality testing
CMG controller failure	EEPROM on CMG controller failure	SFC430 unable to communicate with MDB and read from flash of CMG controller	5	2	10 (Mod)	No IMU data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table 3-7. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
CMG controller failure	Software error	CMG controller unable to obtain IMU measurements and unable to store data	5	4	20 (High)	No IMU data from SwampSat downlink	Run software during testing to ensure algorithm is working
Communication to CMG controller failure	SPI signal error	SFC430 unable to communicate with CMG controller	5	2	10 (Mod)	No IMU data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
IMU ADIS16405 failure	Insufficient power	Unable to take IMU measurements	1	4	4 (Low)	No IMU data from SwampSat downlink	Continuous monitoring and wait until sufficient power
	IMU temperature sensor failure	Unable to downlink temperature data of IMU	1	2	2 (Low)	Unable to obtain IMU temperature data from SwampSat	Functionality testing
IMU ADIS 16405 failure	SPI signal error	CMG controller unable to read IMU data	5	2	10 (Mod)	No IMU data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
	IMU breaks due to environmental conditions	Unable to take IMU reading	5	2	10 (Mod)	No IMU data from SwampSat downlink	Environmental testing before launch
Power failure	Insufficient power	SwampSat unable to operate Detumble mode	1	4	4 (Low)	Unable to operate Detumble mode and SwampSat goes in Safe-Hold	Continuous monitoring and wait until sufficient power
	Components on EPS board malfunction due to environmental conditions	Unable to generate any power for SwampSat	5	2	10 (Mod)	No communication from SwampSat	Environmental testing before launch

Table 3-7. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Communication to EPS board failure	I2C signal error	Unable to obtain the power information from the EPS board	5	2	10 (Mod)	No power information in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
Magnet coils failure	PCB panels failure due to environment conditions	Unable to use magnet coils, no power generation from solar cells	5	2	10 (Mod)	No communication from SwampSat	Environment testing before launch
	Malfunction of the load switch	Unable to generate magnetic field to interact with the Earth's magnetic field	5	2	10 (Mod)	IMU rates are high and the Flag = Failure	Functionality testing before launch
Magnet coils failure	Insufficient magnetic field generation	Unable to detumble due to weak magnetic field generation from magnetic coils	5	2	10 (Mod)	IMU rates are high and the Flag = Failure repetitively	Functionality testing, simulation, and analysis before launch
Data failure	RTC failure	Unable to provide real-time	3	2	6 (Low)	No real-time data in downlink from SwampSat	Run software during testing to ensure algorithm is working
	EEPROM on SFC430 failure	Unable to store data	5	2	10 (Mod)	No data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table 3-7. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Downlink failure	Transmitter failure	SwampSat unable to transmit satellite health data to ground	5	2	10 (Mod)	No satellite health data from SwampSat	Functionality testing before launch
	Query beacon failure	Unable to read telemetry from CMG Controller, EPS board, Transceiver, RTC, Flash, and temperature sensor	4	4	16 (High)	No data from SwampSat downlink	Run software during testing to ensure algorithm is working
	Ground station failure	Unable to receive telemetry from SwampSat	5	1	5 (Mod)	Unable to receive telemetry from SwampSat	Test equipment regularly and functionality testing before launch
Connection failure	Cabling failure	No connection and communication between interfaces	5	3	15 (High)	No communica tion with SwampSat	Ground testing before launch for proper connection between interfaces
Software error in Detumble algorithm	Programming error	Unable to operate Detumble mode, Detumble failure	5	4	20 (High)	No detumble information in SwampSat downlink	Run software during testing to ensure algorithm is working

Both failures could result in the SwampSat mission failure, thus, the severity was ranked as unacceptable (LS5). The SwampSat receiver is made up of COTS components, therefore, the likelihood was assigned as unlikely (LL2). Additionally, the ground station equipment is made up of COTS components, however, the equipment can be regularly monitored and if necessary, different ground station can be used, therefore, the likelihood was assigned as remote (LL1) To prevent the failures, functionality tests will be performed on the receiver as well as the ground station equipment. The ground station equipment will be tested regularly to ensure that the communication is established with SwampSat. Once in the detumble operating mode, the SFC430 will not be able to obtain IMU rates if the CMG controller, the communication link to the CMG controller, or the IMU fails. The CMG controller failure could occur from the malfunction of the EEPROM. If the EEPROM on the CMG controller is unable to store the IMU rates, then the SFC430 will not be able to obtain any IMU rates, thus, severity was assigned as unacceptable (LS5). Another reason that the CMG controller could fail is from software error. If there is software error, the CMG controller will not acquire the IMU rates and will not be able to write to the EEPROM, therefore, the severity was ranked as unacceptable (LS5). The EEPROM on the CMG controller is a COTS component, therefore, the likelihood was listed as unlikely (LL2). However, the software error was evaluated as highly likely (LL4) to fail since all the software is written in-house. As mentioned above, the communication between the SFC430 and the CMG controller is effected through SPI link and if the SPI link fails due to signal error, the SFC430 will not be able to obtain data from the CMG controller, so the severity was chosen as unacceptable (LS5). The SPI is implemented using the standard protocol, therefore, the likelihood of the SPI signal error is viewed as unlikely (LL2). If the CMG controller or the communication to the CMG controller fails, the ground station will not receive any IMU data from SwampSat downlink. To avoid the CMG controller failure caused by the EEPROM malfunction, the EEPROM will be tested for its functionality and the software will be debugged. Running simulations during testing to ensure the communication between the CMG controller and the SFC430 will help reduce the SPI signal error from happening.

The IMU could be another reason for the detumble operation mode fails. The IMU could fail due to insufficient power, SPI signal error, temperature sensor failure, or environmental conditions. If there is insufficient power to power the IMU, no angular rates would be obtained. However, the batteries will be charged to provide power, therefore, the severity was listed as no impact (LS1). Power is very limited in orbit, therefore the likelihood of occurrence was ranked as highly likely (LL4). If the SPI signal failure occurs, the CMG controller will not be able to read the angular rates from the IMU and there will be no IMU data in the SwampSat downlink. Without the IMU data, the ground station will not know what the angular rates of SwampSat are, so the severity was listed as unacceptable (LS5). The likelihood of the SPI signal error was listed as unlikely (LL2) since the SPI will be implemented using standard protocol. As mentioned before, to prevent the SPI signal error from occurring, the software will be simulated during testing to ensure the CMG controller can read from the IMU. The temperature sensor on the IMU can fail, however, not having the temperature sensor data will not cause the SwampSat mission to be a failure so the severity was ranked as no impact (LS1). The IMU itself can break or malfunction due to environmental conditions so the severity was listed as unacceptable (LS5). The IMU on SwampSat is a COTS component from Analog Devices, Inc [34], therefore, the likelihood of the temperature sensor or the IMU itself failing was listed as unlikely (LL2). Functionality tests will be performed on the IMU including running simulations to prevent the IMU from failing. The IMU will also be placed in the thermal vacuum chamber and also on the vibration shaker table to prevent failures from environmental conditions.

Once the program detects that there are differences between the measured angular rates and the predefined rates, the SFC430 commands the magnetic coils to be turned on. However, the magnetic coils failure could occur. The PCB solar panel failures, malfunction of the load switch, or insufficient magnetic field generation could cause the magnetic coils failure. When the PCB solar panels fail, the magnetic field will not be generated since the magnet coils are embedded in the panels. Not only would the magnetic field fail to be generated, the solar cells on the solar panels would not be able to charge the batteries and the SwampSat mission would be a failure. Thus, the severity of this failure was ranked as unacceptable (LS5). The likelihood was ranked as unlikely (LL2) since the PCB solar panels were designed in-house although manufactured outside. Also, functionality tests, observation, and inspection will be performed on the PCB solar panels to avoid the failure from occurring. Detailed FMECA on the solar cells are shown in EPS subsystem FMECA, Appendix B-4. The FMECA for the PCB solar panels are shown in structures FMECA, Appendix B-6. Another cause of the magnet coil failure is the malfunction of the load switch. When the load switch is turned on, it allows the current to pass through to the magnet coils, however, if the switch malfunctions, no current will pass through to generate any magnetic field. The severity of the malfunction of the load switch was ranked as unacceptable (LS5) since with no magnetic field, SwampSat will not be stabilized. The likelihood was ranked as unlikely (LL2) since the load switch is a COTS component. If the magnetic field generated by the magnet coils is insufficient, SwampSat will not stabilize. No stabilization means SwampSat will be unable to perform attitude maneuvers, so the severity was ranked as unacceptable (LS5). The likelihood was ranked as unlikely (LL2) since the amount of magnetic field generated by the magnet coils have been calculated and detumbling analysis has been conducted. Detailed FMECA of the magnetic coils can be seen in the ACS subsystem FMECA, Appendix B-1. As one can see in the software architecture for the detumble mode, the status flag is updated once the magnet coils have been turned on and the IMU rates are measured. If the IMU rates received from SwampSat are high and that the status flag is at “Failure”, either the load switch malfunctioned or the magnetic field generated were insufficient. To prevent the malfunction of the load switch, functionality tests will be performed and to prevent insufficient magnetic field generation, further simulations and analyses will be executed.

The detumble mode uses more power than the safe-hold mode, therefore, the program will query the EPS battery board to ensure sufficient power is present in the batteries to execute the operation. The program will query through Inter-Integrated Circuit (I2C) communication to the EPS board. The power failure could occur during the detumble mode, caused by the insufficient power or the malfunctions of the components on the EPS board. The battery might not have enough charge to provide power to operate the detumble mode. In that case, the program is designed to return to the main operating mode, the safe-hold mode. The battery can be recharged during the safe-hold mode, so the severity was listed as no impact (LS1). Also, since power is very limited, the likelihood of the power failure due to insufficient power was listed as highly likely (LL4). The components on the EPS board could malfunction due to environmental conditions and if that occurs, there will be no communication with SwampSat and the mission is over. Therefore, the severity was listed as unacceptable (LS5). As mentioned earlier, the EPS board is a COTS component from Clyde Space, therefore, the likelihood was ranked as unlikely (LL2). The EPS board will be placed in the thermal vacuum chamber and the vibration shaker table to avoid any possible failures by the environmental conditions. If the I2C signal error occurs, the SFC430 is unable to obtain the power information from the EPS subsystem. The severity was ranked as unacceptable (LS5), since the ground station will not know the power of SwampSat. Like the SPI communication, the I2C is also implemented using standard protocol, therefore, the likelihood was listed as unlikely (LL2). Functionality testing as well as running simulations for the I2C will be conducted to ensure that the I2C communication is established.

Once the measured angular rates are close to the predefined angular rates, the program is designed to record the detumble operation a success as a status flag on to the EEPROM. The detumble mode can be terminated through ground commands or autonomously when the measured angular rates meet the predefined angular rates. During the detumble operation mode, SwampSat is designed to transmit health data at specific intervals. Also, the detumble telemetry will be recorded onto the EEPROM and the recorded telemetry will be transmitted down to the ground station during the Comms operating mode.

As mentioned previously, the data failure could also occur here. The real time clock (RTC) could fail to provide real-time and EEPROM on the SFC430 could fail to store any data for the detumble mode. The severity was ranked as moderate impact (LS3) for RTC failure and unacceptable (LS5) for the EEPROM failure. The likelihood for both failures was listed as unlikely (LL2) since they are both COTS components. Functionality tests and the algorithms would be tested for both to ensure the components are working properly.

Like in the safe-hold mode, the detumble mode is designed to downlink the satellite health data. The transmitter, the ground station, and the query beacon function could fail to cause the downlink failure. The severity for the transmitter failure and the ground station failure was listed as unacceptable (LS5) and the query beacon function failure was ranked as major impact (LS4). The transmitter and the ground station are both developed with COTS components, therefore, the likelihood was ranked as unlikely (LL2). The function query beacon was developed in-house, thus, the likelihood was ranked as highly likely (LL4). The downlink failure could be avoided by performing functionality tests on the transmitter and the ground station equipment and to debug and to run simulations for the query beacon function.

The connection failure and the software error could occur in the detumble operating mode as well. No connection between interfaces would cause not only detumble mode failure but SwampSat mission failure too, so the severity was listed as unacceptable (LS5). The software error in the detumble mode algorithm could also cause the SwampSat mission to be a failure since SwampSat is unable to stabilize, thus, severity was ranked as unacceptable (LS5). The likelihood for the connection failure was ranked as likely (LL3) and the software error likelihood was listed as highly likely (LL4). To avoid connection failure, all the connections will be tested. To prevent any software error, the algorithm will be tested by running simulations to check for any issues with the algorithm.

The high criticality items listed for the detumble mode are the CMG controller failure due to software error, downlink failure due to query beacon failure, connection failure from cabling failure, and software error for the detumble mode due to programming error. Again, not only should the high criticality items must be carefully taken care of, but also the moderate and the low criticality items must be taken into consideration.

3.6 Comms Mode

The Comms mode is designed to downlink mission validating data to the ground. The data to be transmitted to the ground station includes detumble data, Attitude Determination System (ADS) data, and Control Moment Gyroscope Operations (CMG Ops) data. The data are stored on two EEPROM devices located on the SFC430 and the CMG controller. The EEPROM located on the SFC430 stores detumble telemetry data and the EEPROM on the CMG controller stores ADS and CMG Ops telemetry data. Unlike the other operating modes, the Comms operating mode does not have a downlink telemetry data. The telemetry will be transmitted to the ground at shorter intervals than the safe-hold mode, so it requires more power. When the transmitted data is not captured by the ground station, the transmission will be repeated. The software architecture and the FMECA for the Comms operating mode can be seen in Appendix A-5 and in Table 3-7 respectively. Also, the downlink telemetry data for all the operating modes, detumble mode, ADS mode, and CMG Ops mode can be seen in Appendix C.

As in the detumble mode, the Comms mode requires large power to operate, therefore, the program is designed to perform a power check. Depending on which telemetry the ground station invokes, the program is designed to access the telemetry strings on the EEPROMs and to transmit to the ground station.

Table 3-8. Comms mode FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Uplink failure	Receiver failure	SwampSat unable to receive commands from ground station	5	2	10 (Mod)	SwampSat does not respond to ground commands	Functionality testing before launch
	Ground station failure	Unable to uplink commands from ground station to SwampSat	5	1	5 (Mod)	Unable to uplink commands to SwampSat	Test equipment regularly and functionality testing before launch
Power failure	Insufficient power	Unable to operate Comms mode	1	4	4 (Low)	Unable to operate Comms mode and SwampSat goes in Safe-Hold mode	Continuous monitoring and wait until sufficient power
Power failure	Components on EPS board malfunction due to environment conditions	Unable to generate any power for SwampSat	5	2	10 (Mod)	No communication from SwampSat	Environment testing before launch
Communication to EPS board failure	I2C signal error	Unable to obtain the power information from the EPS board	5	2	10 (Mod)	No power information in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
Telemetry failure	I2C signal error	Unable to read Flash storage on SFC430	5	2	10 (Mod)	No information on SwampSat detumble telemetry	Functionality testing and run software during testing to ensure algorithm is working

Table 3-8. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Telemetry failure	EEPROM on SFC430 failure	Unable to access Flash storage on SFC430	5	2	10 (Mod)	No information on SwampSat detumble telemetry	Functionality testing and run software during testing to ensure algorithm is working
	SPI signal error	Unable to read Flash storage on CMG controller	5	2	10 (Mod)	No information on SwampSat ADS and CMG Ops telemetry	Functionality testing and run software during testing to ensure algorithm is working
	EEPROM on CMG controller failure	Unable to access Flash storage on CMG controller	5	2	10 (Mod)	No information on SwampSat ADS and CMG Ops telemetry	Functionality testing and run software during testing to ensure algorithm is working
Downlink failure	Transmitter failure	SwampSat unable to downlink telemetry for each operating mode; SwampSat unable to transmit satellite health data	5	2	10 (Mod)	No telemetry in downlink from SwampSat ; No satellite health data from SwampSat	Functionality testing before launch
	Query beacon failure	Unable to read telemetry from CMG Controller, EPS board, Transceiver, RTC, Flash, and temperature sensor	4	4	16 (High)	No data from SwampSat downlink	Run software during testing to ensure algorithm is working

Table 3-8. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Downlink failure	Ground station failure	Unable to receive telemetry from SwampSat	5	1	5 (Mod)	Unable to receive telemetry from SwampSat	Test equipment regularly and functionality testing
Connection failure	Cabling failure	No connection and communication between interfaces	5	3	15 (High)	No communication with SwampSat	Ground testing before launch for proper connection between interfaces
Software error in Comms algorithm	Programming error	Unable to operate Comms mode, Comms Failure	5	4	20 (High)	No telemetry in downlink from SwampSat	Run software during testing to ensure algorithm is working

Like the other operating modes, satellite health data is transmitted down to the ground station during the Comms mode.

SwampSat will not enter the Comms operating mode if the uplink failure occurs. Either the receiver failure or the ground station failure would cause the uplink failure. If the receiver fails, the commands sent to SwampSat to enter the Comms mode would never be picked up by SwampSat, so the severity was ranked as unacceptable (LS5). Also, if the ground station failure occurs, no commands can be sent to SwampSat, thus, severity was listed as unacceptable (LS5). For the receiver failure, the likelihood was ranked as unlikely (LL2) since it is made up of COTS components. For the ground station failure, the likelihood was assigned as remote (LL1) since it can be regularly monitored and other ground station can be used. Functionality tests will be performed on the receiver and on the ground station equipment to prevent uplink failures.

Once SwampSat receives the command from the ground station to enter the Comms mode, the program will first perform a power check with the EPS subsystem. Power failure occurs when SwampSat has insufficient power or when the components of the EPS subsystem fail due to environmental conditions. When SwampSat has insufficient power, the program will autonomously return to the safe-hold mode. However, SwampSat can wait until sufficient power to re-enter the Comms operating mode, therefore the severity was ranked as no impact (LS1). As mentioned earlier, the Comms operating mode is a power intensive mode, and insufficient power could occur frequently, therefore, the likelihood was ranked as highly likely (LL4). When the components of the EPS board fail, the Comms mode will fail and so will the SwampSat mission; as a result, the severity was ranked as unacceptable (LS5). The components on the EPS board are all COTS components, therefore, likelihood was listed as unlikely (LL2). Environmental testing would be executed to ensure the components of the EPS board will not fail. The I2C signal error results in no power information from SwampSat. Not knowing the power of SwampSat, the ground station will not be able to command SwampSat to perform attitude maneuvers, so the severity was ranked as unacceptable (LS5). The likelihood of I2C signal error was listed as unlikely (LL2), since I2C is implemented using standard protocol. The I2C signal will be tested by running simulations to guarantee communication between the SFC430 and the EPS subsystem.

Once the power check is completed, the program will access the telemetry string on either the SFC430 or the CMG controller. The software architecture for the function access telemetry can be seen in Appendix A-6. The ground station will command either to gather the detumble telemetry data from the SFC430 EEPROM or ADS and CMG

Ops telemetry data from the CMG controller EEPROM. Telemetry failure could occur from I2C signal error, SFC430 EEPROM failure, SPI signal error, or CMG controller EEPROM failure. The I2C signal error will not allow SFC430 to communicate with the SFC430 EEPROM to gather detumble telemetry data. The SFC430 EEPROM failure will result in no detumble telemetry data. For both failures, the severity was ranked as unacceptable (LS5) since the ground station will not receive any detumble telemetry. With the SPI signal error, the SFC430 is unable to communicate with the CMG controller to obtain either the ADS telemetry data or the CMG Ops telemetry data. Also, if the EEPROM on the CMG controller fails, no ADS telemetry data or the CMG Ops telemetry data can be stored. For both of these failures, the severity was ranked as unacceptable (LS5) since the ground station will not receive any information on the ADS telemetry data or the CMG Ops telemetry data. For all of the causes for the telemetry failure the likelihood was ranked as unlikely (LL2). The EEPROMs are both COTS components and the SPI and I2C signals are both implemented using standard protocol, therefore, the likelihood for all were ranked lower. In order to prevent the telemetry failure from happening, functionality tests and software simulations will be conducted for all.

Once the SFC430 gathers the telemetry data, the transmitter will be turned on to downlink the data to the ground station. Like the other modes, the Comms operating mode is also designed to transmit real-time satellite health data. Downlink failure can occur to prohibit SwampSat from transmitting down to the ground station. The downlink failure could be caused by the transmitter failure, the ground station failure, or the query beacon function failure. As mentioned earlier, the transmitter failure leads to no telemetry data or the satellite health data downlink, therefore, the severity was decided as unacceptable (LS5). The ground station failure results in ground station unable to receive telemetry, thus, the severity was ranked as unacceptable (LS5). The query beacon function failure will mean no satellite health data from SwampSat, so the severity was ranked as major impact (LS4). The likelihood for the transmitter failure was listed as unlikely (LL2) since it is made up of COTS components. For the ground station failure, the likelihood was assigned as remote (LL1), since equipment is regularly tested and different ground station can be used. The likelihood for the query beacon function failure was listed as highly likely (LL4) since the algorithm was developed in-house. To prevent downlink failure, the transmitter and the ground station equipment will be tested for their functionality. The software for the query beacon function will be simulated to ensure the function works accordingly.

Similar to the other modes, the connection failure and software error could cause the Comms mode to fail. With no connection between interfaces, the ground station will not have any communication with SwampSat, so severity was ranked as unacceptable (LS5). The software error in the Comms mode will mean the operation of Comms mode is finished, thus severity was ranked as unacceptable (LS5). The likelihood for the connection failure and the software error were ranked as likely (LL3) and highly likely (LL4) respectively. To avoid connection failure, all the connections will be tested. To prevent any software errors, the algorithm will be tested by running simulations to check for any issues with the algorithm.

As in the safe-hold mode, the high criticality items for the Comms mode are downlink failure due to query beacon failure, connection failure from cabling failure, and software error in the Comms mode algorithm due to programming error. Special attention will be needed for these possible failures. Thorough testing procedures and careful planning must be done in order to prevent any of these failures from occurring. There are several moderate criticality items which need to be addressed as well. While the high and the moderate criticality items are attended to, the low criticality items must be considered.

3.7 ADS Mode

The Attitude Determination System (ADS) mode is designed to validate the ADS subsystem by addressing tasks on the SFC430. The ADS mode is also designed to accommodate interaction between the SFC430 and the CMG controller. In order to derive SwampSat's full three-axis attitude, two or more attitude measurements must be processed together. The on-board attitude sensors for SwampSat are the Sun sensors, magnetometer, and the IMU. The ADS program is designed to relay the attitude measurements recorded by the SFC430 to the CMG controller. The attitude determination and attitude estimation algorithms are both hosted on the CMG controller. The attitude determination is done using the quaternion estimation (QUEST) algorithm and Murrell's version of the extended Kalman filter (EKF) is used for the attitude estimation. The QUEST and EKF algorithms will be used to process attitude data. The ADS validation process will first determine the attitude, then filter noise, and propagate. The software architecture for the ADS mode can be seen in Appendix A-7 and the downlink telemetry data is shown in Appendix C-3.

The FMECA for the ADS mode is shown in Table 3-8. Just like the other operating modes, the program will enter the ADS mode when commanded by the ground station. When the uplink failure occurs due to the receiver or the ground station failure, then SwampSat will not be able to enter ADS mode. One of the objectives of the SwampSat mission is to validate the ADS subsystem. If SwampSat is unable to enter and operate the ADS mode, the SwampSat mission would be a failure. Therefore, the severity of the uplink failure can be ranked as unacceptable (LS5). The components on the receiver and the ground station equipment are all COTS components, thus, the likelihood is listed as unlikely (LL2). Functionality tests will be performed on the receiver and the ground station equipment. Furthermore, the ground station equipment can be tested regularly to ensure all the equipment is working accordingly.

Table 3-9. ADS mode FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Uplink failure	Receiver failure	SwampSat unable to receive commands from ground	5	2	10 (Mod)	SwampSat does not respond to ground commands	Functionality testing before launch
	Ground station failure	Unable to uplink commands to SwampSat	5	1	5 (Mod)	Unable to uplink commands to SwampSat	Test equipment regularly and functionalit y testing
Power failure	Insufficient power	SwampSat unable to operate ADS mode	1	4	4 (Low)	Unable to operate ADS mode and SwampSat goes into Safe-Hold	Continuous monitoring and wait until sufficient power
	Components on EPS board malfunction due to environment conditions	Unable to generate any power for SwampSat	5	2	10 (Mod)	No communic ation from SwampSat	Environment testing before launch

Table 3-9. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Communication with EPS board failure	I2C signal error	Unable to obtain the power information from the EPS board	5	2	10 (Mod)	No power data in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
CMG controller failure	EEPROM on CMG controller failure	SFC430 unable to communicate with MBD and read from Flash of CMG controller	5	2	10 (Mod)	No attitude telemetry from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
	Software error	CMG controller unable to execute QUEST and EKF algorithms for ADS validation process	5	4	20 (High)	No attitude telemetry from SwampSat downlink	Run software during testing to ensure algorithm is working
Communication with CMG controller failure	SPI signal error	SFC430 unable to read IMU rates from Flash on; CMG controller unable to initiate ADS validation process	5	2	10 (Mod)	No IMU and quaternion data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
Sun sensor failure	Sun sensor burns out due to radiation damage; environment conditions	Unable to obtain Sun Sensor measurement and sun vector	5	5	25 (High)	No Sun Sensor data from SwampSat downlink	Environment testing before launch
	Sun sensor saturation occurs due to filter failure	Unable to obtain proper Sun Sensor measurement and not able to computer sun vector	5	5	25 (High)	Able to determine that the sun sensor has saturated from SwampSat downlink	Functionality testing before launch

Table 3-9. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
AD converter (SFC 430) failure	ADC signal error	SFC430 unable to read Sun sensor data	5	2	10 (Mod)	No Sun sensor data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
Magnetometer failure	Magnetometer burns out due to power bus spike	SFC430 unable to obtain magnetizer readings to compute magnetic field vector	5	2	10 (Mod)	No magnetometer data from SwampSat downlink	Functionality testing before launch
	Magnetometer breaks due to environment conditions	SFC430 unable to obtain magnetizer readings to compute magnetic field vector	5	2	10 (Mod)	No magnetometer data from SwampSat downlink	Environment testing before launch
AD converter (AD7994) failure	ADC signal error	AD7994 unable to read magnetometer data	5	2	10 (Mod)	No magnetometer data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
Communication with AD7994 failure	I2C signal error	SFC430 unable to read magnetometer measurement	5	2	10 (Mod)	No magnetometer data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
IMU ADIS16405 failure	IMU breaks due to environment conditions	Unable to take IMU reading	5	2	10 (Mod)	No IMU data from SwampSat downlink	Environment testing before launch
Data failure	RTC failure	Unable to provide real-time	3	2	6 (Low)	No real-time data in downlink from SwampSat	Run software during testing to ensure algorithm is working

Table 3-9. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Data failure	EEPROM on CMG controller failure	Unable to store data	5	2	10 (Mod)	No data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
Downlink failure	Transmitter failure	SwampSat unable to transmit satellite health data to ground station	5	2	10 (Mod)	No satellite health data from SwampSat	Functionality testing before launch
	Query beacon failure	Unable to read telemetry from CMG Controller, EPS board, Transceiver, RTC, Flash, and temperature sensor	4	4	16 (High)	No satellite health data from SwampSat	Run software during testing to ensure algorithm is working
	Ground station failure	Unable to receive telemetry fror SwampSat	5	1	5 (Mod)	Unable to receive telemetry from SwampSat	Test equipment regularly and functionality testing before launch
Connection failure	Cabling failure	No connection and communication between interfaces	5	3	15 (High)	No communication with SwampSat	Ground testing before launch for proper connection between interfaces
Software error in ADS algorithms	Programming error	Unable to validate attitude determination subsystem	5	4	20 (High)	No telemetry from SwampSat downlink	Run software during testing to ensure algorithm is working

Once the program enters the ADS mode, the first task is to conduct a power check. Since power is very limited, a power check must be performed to ensure SwampSat has sufficient power to operate the ADS mode. Power failure can be caused by insufficient power or from malfunctions of the components on the EPS board. The malfunction of the components on the EPS board could occur due to environmental conditions. When SwampSat has insufficient power, the ADS mode software is designed to return to safe-hold mode. However, when the components of the EPS board malfunction to provide power, SwampSat will not operate. The severity of insufficient power can be ranked as no impact (LS1) since the batteries can be recharged during safe-hold mode. The malfunction of the EPS board components occurs, the SwampSat mission will be a failure, so the severity is ranked as unacceptable (LS5). As pointed out earlier, the power is very limited, therefore, the likelihood that insufficient power could occur was listed as highly likely (LL4). The components on the EPS board are all COTS parts, thus, the likelihood was listed as unlikely (LL2). The only way to prevent the malfunctions from happening would be to perform environmental testing, using both the thermal vacuum chamber and the vibration shaker table. The power check will not be completed if there were no communication between SFC430 and the EPS board. The communication is done through I2C link and if the I2C signal error occurs, SFC430 will not receive any power information from the EPS board. Also, with the I2C signal error, the ground station will not receive any power information in the downlink from SwampSat. One of the SwampSat mission operations concepts is to validate the EPS subsystem by the power information downlink, so the severity of the I2C signal error was ranked as unacceptable

(LS5). The I2C communication link will be implemented using standard protocol, so the likelihood was listed as unlikely (LL2). The I2C communication link will be tested by running simulations to ensure that the SFC430 can obtain power information from the EPS board.

Once SwampSat has sufficient power to operate the ADS mode, the validation of the ADS subsystem will begin. The SFC430 will command the CMG controller via SPI communication link to initiate the validation process. If the SPI communication fails, the CMG controller will not be able to initiate the ADS validation process. From this, the severity of the SPI signal error was listed as unacceptable (LS5). As mentioned before, the likelihood of the SPI signal error was ranked as unlikely (LL2) since the SPI will be implemented using standard protocol. Simulations and functionality tests will be performed to ensure that the SPI signal failure will not occur. Not only could the SPI communication fail, the CMG controller and the IMU could fail as well. The CMG controller failure could occur from the EEPROM failure or from a software error. As stated before, both the attitude determination and estimation algorithms are hosted on the CMG controller. First, the CMG controller will execute the EKF algorithm and the algorithm is designed to request for Sun sensor and magnetometer measurements from the SFC430. The SFC430 will read six Sun sensor data from the analog-to-digital converter (ADC) on the SFC430. Next the SFC430 will acquire three magnetometer readings from an external ADC via I2C signal. With the measurements, the SFC430 will compute the Sun vector and the magnetic vector and convey them to the CMG controller. If the EEPROM on the CMG controller fails, the body vector measurements from SFC430 will not be stored and the CMG controller will not be able to use the measurements in the ADS algorithms. For that reason, the severity of the EEPROM failure was ranked as unacceptable (LS5). However, the likelihood was evaluated as unlikely (LL2) since the EEPROM is a COTS component and functionality tests and simulations would be conducted to ensure the EEPROM will function accurately. If the software error occurs, the CMG controller will not be able to execute EKF and the QUEST algorithms causing the ADS mode to fail and the ADS subsystem will not be validated. Thus, the severity of the software error was ranked as unacceptable (LS5). Again, the software for the SwampSat mission has been written in-house, therefore, the likelihood was decided as highly likely (LL4). The only way to prevent software error would be to run simulations to ensure the algorithm provides the proper outcome.

Failure to compute body vector measurements could cause the ADS mode to fail. The Sun sensors could burn out from radiation damage and the SFC430 will not be able to obtain Sun sensor measurements. Also, should the filters on the Sun sensors fail, saturation of the Sun sensor measurements would occur. For both, the severity of the failures was ranked as unacceptable (LS5) since the sun vector will not be computed. The likelihood of the failures was decided as near certainty (LL5) since the Sun sensors are built in-house. To prevent radiation damage, the Sun sensors will be put through environmental testing, thermal and vibration testing. To prevent saturation, the filters will be tested and will be replaced with different filters if necessary.

The magnetometer failure could occur due to power bus spike or from environmental conditions. The magnetometer could burn out from a power bus spike and the magnetometer could break or malfunction from environmental conditions, not allowing the SFC430 to obtain magnetometer readings to compute the magnetic field vector. The severity for both failures was ranked as unacceptable (LS5). The magnetometer on SwampSat is a device from Honeywell Inc [34], therefore, the likelihood for both were decided as unlikely (LL2). When the magnetometer fails, the ground station will not receive any magnetometer readings from the SwampSat downlink. To prevent the magnetometer from burning out, functionality tests will be conducted and to prevent magnetometer malfunction, environmental testing, thermal and vibration testing, will be performed.

Both the Sun sensors and the magnetometer provide analog measurements, therefore, ADC will be used to convert the measurements to digital signals. The ADC on the MSP 430 converts the Sun sensor readings and for the magnetometer readings, an external ADC, AD7994 from Analog Devices, Inc [36], will be used. If the ADC on the MSP 430 fails, the sun vector will not be computed, and magnetic field vector will not be computed if the external ADC fails. The ADC on the MSP 430 and the AD7994 could fail due to ADC signal error. The severity of the ADC signal errors was ranked as unacceptable (LS5) since no body vectors would be computed. The likelihood of the ADC failures was ranked as unlikely (LL2) since both the devices are COTS components and are both easily programmed. Functionality tests and the software will be tested to ensure the ADC signal error would not occur. The SFC430 will have to communicate to the AD7994 via I2C to obtain the magnetometer readings. If the communication fails due to I2C signal error, the SFC430 will not be able to compute the magnetic field vector, thus, the severity was decided as unacceptable (LS5). However, as mentioned before, the I2C will be implemented using standard protocol, therefore, the likelihood was ranked as unlikely (LL2).

Once the CMG controller obtains the sun vector and the magnetic field vector from the SFC430, the attitude determination will begin. The QUEST algorithm is design to determine the initial attitude of SwampSat using the body vectors and the reference vectors from the mathematical models implemented on the CMG controller. The QUEST algorithm is programmed within the EKF algorithm. Once the initial attitude has been determined, the EKF algorithm is designed to filter any noisy measurements. Next, the program is designed to propagate using the IMU. If the IMU malfunctions due to environmental conditions, attitude propagation would not occur, thus, the severity was ranked as unacceptable (LS5). As mentioned, the IMU is a COTS component, therefore, the likelihood was decided as unlikely (LL2). Environmental testing will be conducted to prevent any IMU malfunctions from taking place.

Data failure could occur in the ADS operating mode. All the attitude data will be stored on the EEPROM on the CMG controller. If the EEPROM fails, no attitude data will be received from SwampSat, so the severity of the EEPROM failure was ranked as unacceptable (LS5). As mentioned before, the EEPROM is a COTS component, therefore, the likelihood of the EEPROM failure was decided as unlikely (LL2). Functionality tests and simulations will be conducted to prevent the EEPROM from malfunctioning. If the RTC fails, there will be no real-time received from SwampSat downlink. However, the RTC failure will not cause the ADS mode to fail, therefore, the severity was ranked as moderate impact (LS3). Again, the RTC is a COTS component, thus, the likelihood was ranked as unlikely (LL2). To prevent RTC failure, simulations will be performed to ensure the RTC will provide the real-time.

Just like the other operating modes, the ADS mode is designed to downlink SwampSat's health data during the operation. Downlink failure could occur from transmitter failure, ground station failure, and query beacon failure. The transmitter failure will not allow SwampSat to transmit the satellite health to the ground. The ground station failure will result in no telemetry received from SwampSat. For both failures, the severity was ranked as unacceptable (LS5), however, the likelihood was decided as unlikely (LL2) and remote (LL1) for the transmitter and the ground station, respectively. Functionality tests will be carried out on the transmitter to prevent it from failing in space. On the other hand, the ground station equipment can be tested regularly to ensure no failure on the equipment. The SFC430 will not be able to obtain SwampSat's health data if the query beacon function fails. Although the ground station might not receive SwampSat's health data, the SwampSat mission will not necessarily result in a failure, therefore, the severity was ranked as major impact (LS4). The query beacon function is complex and designed in-house, thus, the likelihood was ranked as highly likely (LL4). Accurate debugging and simulations on the query beacon function will help prevent software errors.

Connection failure and software error in the ADS algorithm could take place as well. If connection failure caused by cabling failure occurs, the ground station will not receive any communication from SwampSat, thus, severity was decided as unacceptable (LS5). All the cabling is done in-house, therefore, the likelihood was ranked as likely (LL3). Each connection will be tested to ensure that the connection failure will not happen. The software error in the ADS algorithm will result in ADS mode failure, which also means that the ADS subsystem will not be validated, thus, severity was ranked as unacceptable (LS5). The software is designed and developed in-house, therefore, the likelihood was chosen as highly likely (LL4). Simulations and debugging will ensure that the ADS algorithm will function properly.

Looking at the ADS mode FMECA, there are several high criticality item which are CMG controller failure due to software error, Sun sensor failure due to radiation damage or saturation, downlink failure due to query beacon failure, connection failure due to cabling failure, and the software error for ADS mode due to programming error. Apart from the Sun sensor failure, the other high criticality items have been mentioned in the other operating modes. The Sun sensor is a crucial component for the SwampSat mission and since the Sun sensors are built in-house, absolute care must be taken in their design and development. Full tests on the Sun sensors would be required. As mentioned time after time, the priority would be to address the high criticality items, however, the moderate and the low criticality items must never be overlooked as well.

3.8 CMG Ops Mode

The control moment gyroscope operations (CMG Ops) mode is designed to validate the attitude control system (ACS) subsystem. The CMG Ops is the most power intensive operation in the SwampSat mission, therefore, the transmitter is completely turned off. However, the receiver will remain on so that the ground commands can be picked up by SwampSat. The uplink from the ground station commands the maneuver type and the maneuver time. Just like the ADS mode, the CMG Ops mode is designed to establish the communication link between the SFC430 and the CMG controller via SPI. The attitude data will be communicated to the CMG controller and along with the attitude determination and attitude estimation algorithms, the CMG control and singularity avoidance algorithms will also be executed. The software architecture for the

CMG Ops mode is listed in Appendix A-8 and the downlink telemetry data can be seen in Appendix C-4.

The FMECA for the CMG Ops mode can be seen in Table 3-10. Like the other modes, the ground station will command SwampSat to enter the CMG Ops mode. The uplink failure, caused by receiver failure or ground station failure, will not let SwampSat enter the CMG Ops mode. No commands will be received if the receiver fails and no commands will be sent to SwampSat if the ground station fails. For both failures, the severity was ranked as unacceptable (LS5). The receiver and the ground station are both composed of COTS components. The likelihood of the receiver failure was chosen as unlikely (LL2) since it is made up of COTS components. The likelihood of the ground station failure was chosen as remote (LL1) since if equipments fail, a different ground station can be used. Functionality tests will help prevent the receiver from failing and the equipment in the ground station will be tested regularly to avoid any kind of ground station failures.

Table 3-10. CMG Ops mode FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Uplink failure	Receiver failure	SwampSat unable to receive commands from ground station	5	2	10 (Mod)	SwampSat does not respond to ground commands	Functionality testing before launch
	Ground station failure	Unable to uplink commands from ground station to SwampSat	5	1	5 (Mod)	Unable to uplink commands to SwampSat	Test equipment regularly and functionality testing

Table 3-10. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Power failure	Insufficient power	SwampSat unable to operate CMG Ops mode	1	4	4 (Low)	Unable to operate CMG Ops mode and SwampSat goes in to Safe-Hold mode	Continuous monitoring and wait until sufficient power
Communication with EPS board failure	Components on EPS board malfunction due to environment conditions	Unable to generate any power for SwampSat	5	2	10 (Mod)	No signal from SwampSat	Environment testing before launch
	I2C signal error	Unable to obtain the power information from the EPS board	5	2	10 (Mod)	No power information in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
Attitude data failure	IMU failure	Unable to obtain angular rates from IMU	5	2	10 (Mod)	No IMU rates from SwampSat downlink	Functionality testing before launch
	SPI signal error	CMG controller unable to obtain IMU rates; SFC430 unable to communicate with CMG controller	5	2	10 (Mod)	No IMU rates from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
	I2C signal error	SFC430 unable to read magnetometer readings from AD7994	5	2	10 (Mod)	No attitude telemetry from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table 3-10. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Attitude data failure	Sun sensor failure	Unable to obtain Sun sensor measurement and not able to compute Sun vector	5	5	25 (High)	No attitude telemetry from SwampSat downlink	Functionality testing before launch
	Magnetometer failure	Unable to obtain magnetometer measurement and not able to compute magnetic field vector	5	2	10 (Mod)	No attitude telemetry from SwampSat downlink	Functionality testing before launch
	AD converters failure	Unable to convert analog signals into digital signals	5	2	10 (Mod)	No attitude telemetry from SwampSat downlink	Functionality testing and simulation before launch
	Software error	CMG controller unable to execute QUEST, EKF, CMG control, and singular avoidance algorithms	5	4	20 (High)	No attitude telemetry from SwampSat downlink	Run software during testing to ensure algorithm is working
CMG failure	Flywheel failure	Unable to perform CMG maneuver	5	5	25 (High)	No flywheel speed from SwampSat downlink	Functionality testing before launch
	Gimbal failure	Unable to perform CMG maneuver	5	5	25 (High)	No gimbal rate and gimbal angle data from SwampSat downlink	Functionality testing before launch
Attitude maneuver failure	CMG controller failure	Unable to perform CMG maneuver; Unable to read/write to EEPROM	5	4	20 (High)	No CMG data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table 3-10. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Attitude maneuver failure	CMG pyramid configuration breaks due to environment conditions	Unable to perform attitude maneuver	5	5	25 (High)	SwampSat unable to perform CMG maneuver	Environmental testing before launch
	CMGs do not produce enough torque	Unable to perform rapid retargeting and precision pointing	5	5	25 (High)	SwampSat unable to perform CMG maneuver commands from ground	Functionality testing and simulation before launch
Data failure	RTC failure	Unable to provide real-time	3	2	6 (Low)	No real-time data in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
	EEPROM on CMG controller failure	Unable to store data	5	2	10 (Mod)	No data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
Connection failure	Cabling failure	No connection and communication between interfaces	5	3	15 (High)	No communication with SwampSat	Ground testing before launch for proper connection between interfaces
Software error in CMG Ops algorithm	Programming error	Unable to operate CMG Ops mode	5	4	20 (High)	No telemetry from SwampSat downlink	Run software during testing to ensure algorithm is working

Once SwampSat receives commands from the ground station and enters the CMG Ops mode, a power check will be conducted. The SFC430 will read the power information from the EPS board via I2C. Power failure could occur when SwampSat has insufficient power or if the components of the EPS board malfunctions. For insufficient power, the program is designed to ensure the CMG controller is turned off and to return to safe-hold mode to recharge the batteries. The ground station can command SwampSat to operate the CMG Ops mode when SwampSat has sufficient power, so the severity was ranked as no impact (LS1). Since power is very limited and the CMG Ops mode is the most power intensive operation, lack of power will be common during the SwampSat mission, therefore, the likelihood was decided to be highly likely (LL4). The components on the EPS board could malfunction due to environmental conditions. In that case, the EPS subsystem will not be able to provide any power for SwampSat and the SwampSat mission will be over, therefore, the severity was ranked as unacceptable (LS5). Though the severity was ranked high, the likelihood was ranked as unlikely (LL2) since the components on the EPS board are all COTS components. Environmental, thermal and vibration, testing will be performed to ensure no components will malfunction during the mission. If I2C signal error occurs, the SFC430 will not be able to obtain any power information and will not execute the CMG Ops mode, thus, the severity was ranked as unacceptable (LS5). However, the I2C is implemented using standard protocol, therefore, the likelihood was ranked as unlikely (LL2).

Once the power check is completed, the SFC430 will command the CMG controller to initiate the ACS validation process. Just like the ADS mode, the CMG controller will execute the QUEST and the EKF algorithms and request the SFC430 to communicate the Sun vector and the magnetic field vector. The CMG controller will read from the IMU to obtain the angular rates. The attitude data failure could occur if the Sun sensors, magnetometer, ADCs, or IMU fails. Also, the I2C signal error, SPI signal error, and the software error could occur to cause attitude data failure. As mentioned in the ADS mode, there are six Sun sensors and one magnetometer on SwampSat. The Sun vector can be computed from the Sun sensor measurements and the magnetic field vector can be computed from the magnetometer readings. If any of the two sensors fail, the attitude will not be determined, therefore, the severity was ranked as unacceptable (LS5) for both. The Sun sensors are designed and developed in-house, therefore, the likelihood was ranked as near certainty (LL5), however, the magnetometer is a COTS component, and thus the likelihood was ranked as unlikely (LL2). To avoid the sensors from failing, functionality tests will be conducted. The sensors will be no use if the ADCs fail. As mentioned earlier, there are two ADCs on SwampSat, one for the Sun sensor measurements and the other one for the magnetometer measurements. For the ADCs, the severity was ranked as unacceptable (LS5) however, both are COTS components and both can be simply programmed, the likelihood was ranked as unlikely (LL2). To prevent ADCs from any failure, functionality tests and simulations will be executed during testing. The SFC430 will obtain magnetometer readings from the ADC via I2C signal. If the I2C signal error occurs, the SFC430 will not be able to compute the magnetic field vector, thus, the severity was ranked as unacceptable (LS5). On the other hand, the likelihood was ranked as unlikely (LL2), since the I2C can be easily implemented using standard protocol. SPI signal error could cause no communication between the SFC430 and the CMG controller. Also, the SPI signal error will lead to the CMG controller not reading from the IMU. For that reason, the severity of the SPI signal error was ranked as unacceptable (LS5). However, like the I2C, the SPI can be programmed using standard protocol, therefore, the likelihood was ranked as unlikely

(LL2). Functionality tests and simulations will help avoid I2C and SPI signal errors. The IMU failure would result in no angular rates which could cause attitude data failure, therefore, the severity was ranked as unacceptable (LS5). The IMU is a COTS component, therefore, the likelihood was decided as unlikely (LL2). The IMU will be tested for its functionality to prevent any failures from occurring.

While executing the ADS algorithms, the CMG control and singular avoidance algorithms will also be executed. The CMG failure could occur when the flywheel or the gimbal fails. For both failures, the severity was ranked as unacceptable (LS5) since if either of the two fails, SwampSat will be unable to perform CMG maneuvers. The CMG has been designed and developed in-house, therefore, the likelihood of failure was ranked as near certainty (LL5). CMG functionality tests will be conducted to ensure CMG failures will not occur. Other attitude maneuver failures could occur when the CMG controller fails, CMG pyramid configuration breaks, or if the CMGs do not produce enough torque. The CMG controller failure would result in no CMG maneuver and no communication with the EEPROM. If the CMG controller fails, the SwampSat mission is over, therefore, the severity was ranked as unacceptable (LS5). As mentioned earlier, the CMG controller failure could occur from software error, therefore the likelihood was ranked as highly likely (LL4). Functionality tests and simulations of the software on the CMG controller will prevent it from failing. When the CMG pyramid configuration breaks due to environmental conditions, the CMG maneuver will not be completed, thus, the severity was ranked as unacceptable (LS5). Again, the CMGs were designed and developed in-house and there is no data to prove that the pyramid configuration will withstand the environmental conditions, thus the likelihood was ranked as near certainty

(LL5). To prevent the configuration from failing, environmental, thermal and vibration, testing will be performed to ensure the pyramid will stay intact. If the CMGs do not produce enough torque, the objective of rapid retargeting and precision pointing (R2P2) will not be accomplished. So, the severity was ranked as unacceptable (LS5). The likelihood was ranked as near certainty (LL5) since the CMGs have no flight heritage to show that the CMGs will produce sufficient torque. Thorough analysis and simulations must be conducted to ensure the CMGs will provide sufficient torque for the mission. Details of the ACS subsystem FMECA can be seen in Appendix B-1.

Once SwampSat performs attitude maneuvers, the attitude data will be stored on the CMG controller EEPROM. The stored data will be transmitted to the ground station during the Comms operating mode. When the RTC fails to provide real-time during the CMG Ops mode, the ground station will not receive any time information from the downlink. Not knowing the real-time will not cause the SwampSat mission to be over, therefore, the severity was ranked as moderate impact (LS3). However, if the CMG controller EEPROM fails, no data will be stored, and the ground will receive no data from the downlink. One of the objectives for the SwampSat mission is to downlink attitude and CMG data, therefore, the severity of the CMG controller EEPROM failure was ranked as unacceptable (LS5). The RTC and the EEPROM are both COTS components, so, the likelihood of failure was ranked as unlikely (LL2). To prevent the RTC and the EEPROM from failing, functionality tests and the software will be simulated thoroughly.

Like the other operating modes, connection failure and software error could cause the CMG Ops mode to fail. The connection failure could be caused by cabling failure and if it happens, the ground station will not receive any communication from SwampSat, thus, the severity was ranked as unacceptable (LS5). The cabling for SwampSat is done in-house, therefore, the likelihood was decided as likely (LL3). To prevent any cabling failures, each connection will be tested before launch. The software error in the CMG Ops mode will imply that SwampSat will not be able to perform CMG maneuvers, therefore, the severity was ranked as unacceptable (LS5). As stated earlier, all the software are designed and developed in-house, therefore, the likelihood of failure was decided as highly likely (LL4). Simulations and debugging will ensure that the CMG Ops algorithm functions properly.

Looking at the FMECA for the CMG Ops mode, the high criticality items are attitude data failure caused by Sun sensor failures or software error, CMG failure due to flywheel failure or gimbal failure, attitude maneuver failure due to CMG controller failure or CMG pyramid configuration failure or not enough torque, connection failure due to cabling failure, and the software error in the CMG Ops mode due to programming error. The main focus for this mode should be the CMGs. The main objective for the SwampSat mission is to validate the CMGs in flight. The CMGs have been designed and developed in house, therefore, multiple tests must be conducted to ensure the CMGs will operate in flight.

3.9 Summary

In summary, detailed FMECA was done for the SwampSat mission. Not all possible failures of SwampSat were identified in the SwampSat mission FMECA. For that reason, in depth FMECA was done for each subsystem to discover other possible failures. The subsystems that were analyzed were ACS, ADS, CDH, EPS, TT&C, and structures. The FMECA for each subsystems are all shown in Appendix B.

The launch stage was not the main focus of the FMECA due to the fact that the SwampSat team has no control. The main focus of the SwampSat FMECA was the SwampSat operating modes. The high criticality failure modes that were identified in each operating modes and brief potential mitigation plans will be discussed here.

In the deployment/startup stage, the following high criticality failure modes were identified; deployment failure from P-POD due to premature antenna deployment, startup failure due to CDH failure, antenna deployment failure due to burn wire mechanism failure or antenna system failure, connection failure due to cabling failure, and software error in the deployment/startup stage due to programming error. The premature antenna deployment and the burn wire mechanism failures can potentially be mitigated by performing antenna deployment tests. The antenna system can be placed on a vibration shaker table to test if the antenna system will withstand any acoustic shocks or vibrations. Additionally, the antenna system can be placed inside a thermal vacuum chamber for thermal cycle testing to ensure that the antenna system will not fail from thermal conditions. The burn wire mechanism can be tested after the vibration testing and also after the thermal testing to ensure the antennas will be deployed. Also, the burn wire mechanism can be tested inside a vacuum for additional assurance. The CDH failure could potentially be prevented by performing multiple tests. The SFC430 can be placed on a vibration shaker table and in a thermal vacuum chamber to ensure that the SFC430 will not break due to environmental conditions. Functionality test of the SFC430 will be conducted before and after the environmental testing. Another test that needs to be performed will be the connection tests to prevent any connection failures. All the cabling will be done in-house, therefore, each connection can be tested. To secure each connection, a layer of epoxy could be added to prevent the connection from becoming loose. Software error must be prevented for the SwampSat mission to be successful. The algorithm will be carefully debugged and simulations of the deployment/startup stage will be performed to ensure there are no programming errors.

In the safe-hold mode, the following high criticality items were identified; downlink failure due to query beacon failure, connection failure due to cabling failure, and software error in the safe-hold algorithm due to programming error. As previously mentioned, the cabling failure can be prevented by testing each connection and by adding a layer of epoxy to prevent the connections from getting loose. Furthermore, the software for the safe-hold mode can be thoroughly debugged and can be simulated to ensure no programming error occurs. Similarly, the query beacon function can be carefully debugged and simulated to ensure that the program can gather the health data.

The high criticality failure modes in the detumble mode were identified as; CMG controller failure due to software error, downlink failure due to query beacon failure, connection failure due to cabling failure, and software error in the detumble algorithm due to programming error. The software on the CMG controller can be debugged and simulated to ensure that the CMG controller can gather the IMU data. As discussed previously, the software, query beacon and algorithm for detumble mode, can be carefully debugged and simulated to ensure they function properly. In addition, each connection will be tested and a layer of epoxy can be added to prevent any cabling failure.

The high criticality failure modes that were identified for the Comms mode were the same as the high criticality failure modes of the safe-hold mode; downlink failure due to query beacon failure, connection failure due to cabling failure, and software error in the Comms mode algorithm. The potential mitigations for those failures are; careful debugging and simulations for the software query beacon and Comms mode algorithm and test each connection and add a layer of epoxy to the connections.

The high criticality items identified in the ADS mode were; CMG controller failure due to software error, Sun sensor failure due to radiation, Sun sensor saturation due to filter failure, downlink failure due to query beacon, connection failure due to cabling failure, and programming error in the ADS mode algorithm. The software on the CMG controller can be carefully examined and simulated to ensure the algorithms can perform attitude determination and attitude estimation. To prevent any radiation damage on the Sun sensors, the Sun sensors can be placed inside the thermal vacuum chamber and to test the functionality afterwards. The Sun sensor filters can be tested by shining a light directly at the Sun sensors to see if any saturation has occurred and replaced if necessary. The software, query beacon and the algorithm for the ADS mode, can be debugged and simulated carefully to prevent any programming error. Each of the connections can be tested and a layer of epoxy can be added to avoid any potential connection failures.

The following lists the high criticality failure modes that were identified in the CMG Ops mode; attitude data failure due to Sun sensor failure or software error, CMG failure due to the flywheel failure or the gimbal failure, attitude maneuver failure due to CMG controller failure, pyramid configuration failure, insufficient torque, connection failure due to cabling failure, and software error in the CMG Ops algorithm. The Sun sensor failure can be prevented by performing functionality and environmental testing. The software will be debugged and simulated to ensure that the attitude data can be obtained by the sensors. Functionality and environmental testing can be performed on the CMGs to prevent any failures. Additionally, the flywheel and the gimbal can be individually tested for its functionality to prevent any failure. Environmental testing and running software for the CMG controller can potentially mitigate possible CMG controller failure. Once the CMGs are assembled into a pyramid configuration, the assembly can be put through vibration and thermal testing, to ensure that the assembly will remain in one piece. Further simulations and analyses can be performed on the CMGs to ensure sufficient torque can be generated for maneuvers. Unlike the other operating modes, the CMG Ops mode is designed to turn off the transmitter to conserve power, therefore, the downlink failure is not listed. However, the connection failure and software error were identified as the high criticality failures modes. As previously stated, to prevent connection failure, each connection can be tested and a layer of epoxy can be placed on the connections. Also, the software for the CMG Ops mode can be carefully debugged and simulated to ensure the algorithm will run appropriately.

The FMECA identified failure modes and their consequences for the SwampSat mission. By using the criticality analysis, each failure modes were ranked according to their risks. Brief preventative actions were listed for each of the failure modes, however thorough analyses and planning must be conducted to develop improved mitigation plans. The high criticality items that were identified were; Sun sensors, CMGs, antenna system, and software. These potential high criticality failure modes were all identified as built in-house components, therefore, priority for the SwampSat team will be to address these built in-house components. However, the lower criticality potential failure modes, the moderate and the low criticality potential failure modes, must also be attended to carefully. The high severity failure modes from the SwampSat FMECA were used to develop the Fault Tree Analysis (FTA) of SwampSat. The SwampSat FTA was created to analyze further the root causes of the potential failures. The SwampSat FTA can be seen in Chapter 4.

CHAPTER 4
SWAMPSAT FTA

Another type of reliability analysis conducted on SwampSat was the Fault Tree Analysis (FTA). As stated before, the FTA complements the Failure Modes, Effects, and Criticality Analysis (FMECA) by starting with the top level failure effect and tracing the failure to potential causes. The FTA identifies individual or collective lower level failures that cause the top level failure. The SwampSat FTA was constructed using Microsoft ® Power Point since the cost of the software was beyond the budget for this project. The SwampSat FTA was applied to the most severe failure effects that cause the SwampSat mission to fail. Like the SwampSat FMECA, the SwampSat FTA was also divided into seven stages; launch, deployment/startup, safe-hold mode, detumble mode, Comms mode, ADS mode, and CMG Ops mode. The SwampSat mission FTA is shown in Figure 4-1.

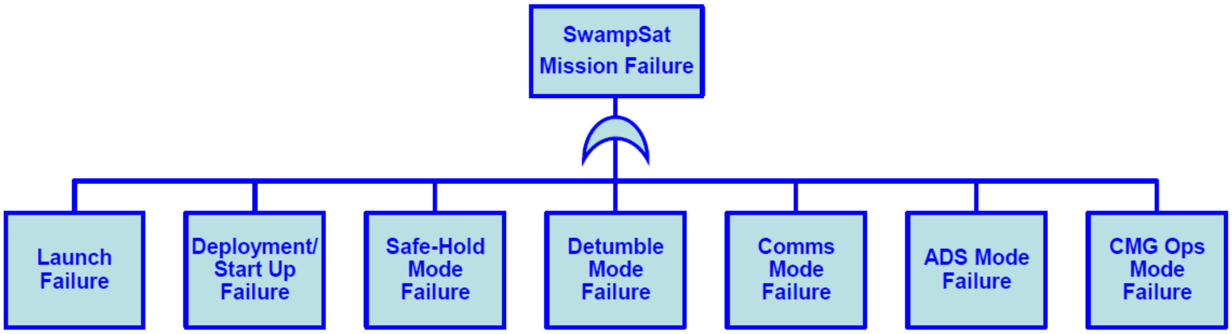


Figure 4-1. SwampSat mission FTA

4.1 Launch Stage FTA

The launch stage looks into before and during launch. Once SwampSat becomes ready for flight, it will be placed inside the P-POD. The P-PODs will be loaded on to the launch vehicle and await launch. Several possible launch failures were identified from the FMECA.

The launch stage FTA can be seen in Figure 4-2. Launch failure can be caused by one of the following; Remove Before Flight (RBF) pin failure, launch vehicle failure, or P-POD failure. The RBF pin failure could occur from a mechanism failure denoted as a circle, which represents the lowest possible cause of failure. The launch vehicle could break due to environmental conditions or burn up during launch. Again, the possible launch vehicle failures were represented as a circle, since the failures were the lowest level failures. The P-POD failure could occur if it breaks due to environmental conditions or if it burns up during launch. The two possible P-POD failures were denoted as the basic failure events.

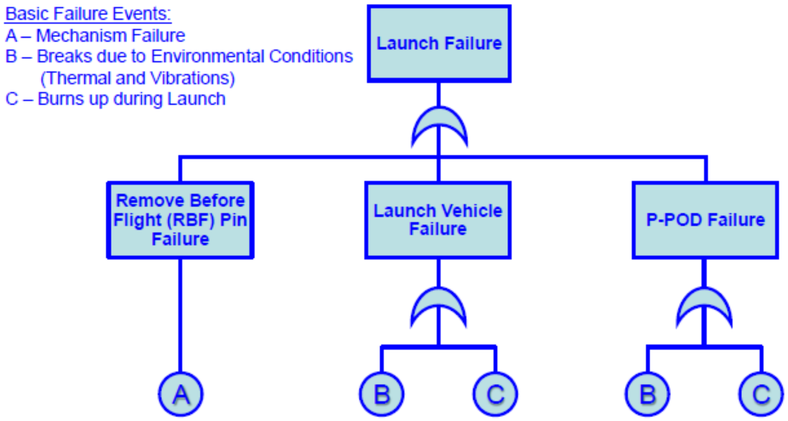


Figure 4-2. Launch stage FTA

Once the basic levels of failures were identified, the critical paths were visual. In the launch stage, the mechanism failure of the RBF pin, rupture due to environmental conditions, or burning up could cause the launch stage to fail, which leads to the SwampSat mission to fail. The launch vehicle is the launch service provider's (LSP's) responsibility, therefore, the SwampSat team has no control. Additionally, the P-POD is Cal Poly's responsibility, thus, the SwampSat team has no control.

4.2 Deployment/Startup FTA

As mentioned in Chapter 3, the deployment/startup stage occurs after launch. After successful launch, the P-PODs carrying SwampSat and other CubeSats will be deployed into orbit. Once SwampSat is ejected out from the P-POD, the antennas will be deployed and the EPS and the CDH subsystems for SwampSat will be powered up upon completion of the wait period. The deployment/startup FTA was developed using the FMECA for the deployment/startup stage.

The FTA for the deployment/startup stage is shown in Figure 4-3. As discussed in the FMECA for the deployment/startup stage, there are several failures that could cause the failure. Deployment failure could occur from either P-POD or from antenna deployment failures. Startup failure could be caused by four lower level failures. The identified failures were; separation switch failure, EPS subsystem failure, CDH subsystem failure, or dead battery. The continuation symbols, denoted as a triangle, were used to describe a more complex system. The continuation symbols were used for the antenna system, data storage, EPS subsystem, and CDH subsystem. The FTA for the antenna system and the data storage are shown in Figure 4-4. Figures 4-5 and 4-6 show the FTA for the EPS and the CDH subsystems respectively.

The deployment failure from the P-POD was analyzed further to determine that the deployment spring, P-POD door, or the environmental conditions could cause the SwampSat's deployment from the P-POD to fail. The failure due to environmental condition could not expand further, therefore, the failure was shown as a basic failure event. The deployment spring and the P-POD door could fail due to mechanism issues, so, the mechanism failure was assigned as the basic failure.

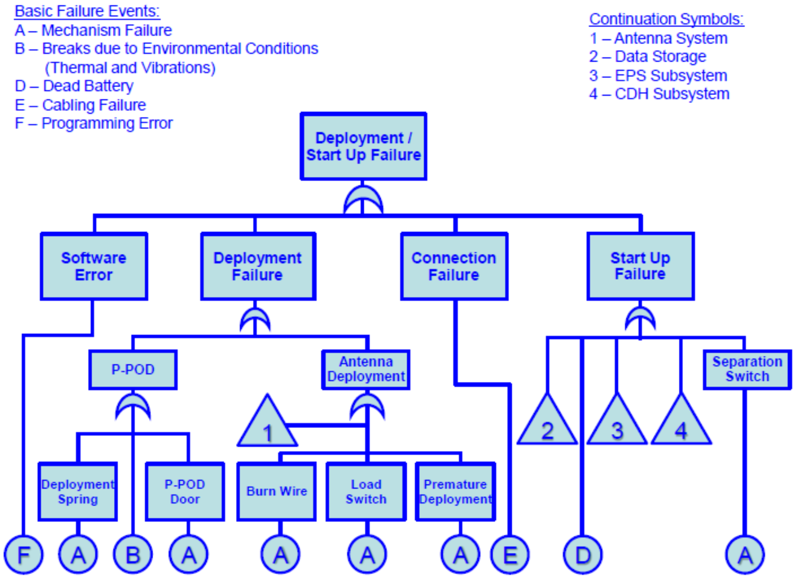


Figure 4-3. Deployment/Startup stage FTA

The antenna deployment failure could happen when failures to antenna system, burn wire, or load switch occurs. Also, the antennas could prematurely deploy while inside the P-POD to cause the antenna deployment failure. Mechanism failure could cause the burn wire and the load switch to fail and also cause premature antenna deployment. Mechanism failure could not expand further, therefore, it was given the basic failure event. The antenna system could be extended more, therefore, the continuation symbol was used.

Following successful antenna deployment, the EPS and the CDH subsystems will be powered up. As briefly explained, the startup failure level can be expanded more to investigate possible failures. Separation switch failure was one of the lower level failures that could cause startup failure. The separation switch could only fail due to mechanism failure. The EPS and the CDH subsystems were also identified as lower level failures of startup failure. The two subsystems could be analyzed further, therefore, the continuation symbols were used. A dead battery would be another cause of startup failure and since it cannot be expanded further, the basic failure event symbol was assigned.

Once the CDH subsystem is powered up, the main flight computer, SFC430, will read the time from the real-time clock (RTC) and store that data in the Electronically Erasable and Programmable Read Only Memory (EEPROM). Further analyses were done on the RTC and the EEPROMs, therefore they were denoted as data storage continuation symbol.

Software error and connection failures were also identified as possible failures for the deployment/startup stage. Software error could only occur from programming error and connection failure could only happen due to cabling error. Both were identified as the basic failure events that could cause the deployment/startup failure.

The basic failure events identified for the deployment/startup stage were; mechanism failure, environmental conditions, dead battery, cabling failure, and programming error. Using these basic failure events, preventative actions and mitigation plans can be developed to avoid the possibility of deployment/startup failure.

4.2.1 Antenna System FTA

The antenna system was expanded to examine possible failures. Looking at the FMECA for the antenna system, three lower levels were identified. Receive and transmit antenna module failures were represented as events that lead to other lower level failures. The failure from environmental conditions was denoted as a basic failure for one of the antenna system failures. The receive and transmit antenna modules consist of a delrin plate, nitinol dipole antenna elements, antenna deployment mechanism, and interfaces. The antenna deployment mechanism was not considered as a part of the antenna system since the antenna deployment was covered in the deployment/startup stage. For both antenna modules, failures to the delrin plate, the nitinol dipole antenna elements, or the interfaces could cause the modules to fail. The delrin plate and the antenna elements were represented as basic failure events, however, the interface was denoted as an event since cabling failure was identified as a lower level to the interface failure that could cause the antenna system failure.

4.2.2 Data Storage FTA

The data storage failure could occur from EEPROM failure, RTC failure, or software error. As stated in the Chapter 3, SwampSat has two EEPROM devices, one on the SFC430 and one on the CMG controller, therefore, the EEPROM failure was expanded into two events. SFC430 EEEPROM could fail due to environmental conditions or I2C signal error. CMG controller EEPROM could fail due to environmental conditions or SPI signal error. The RTC failure could be caused by either the environmental conditions or from I2C signal error, thus, denoted as basic failures. The environmental conditions could cause the components to break or malfunction. The software error could only occur due to programming error, so the basic failure symbol was decided.

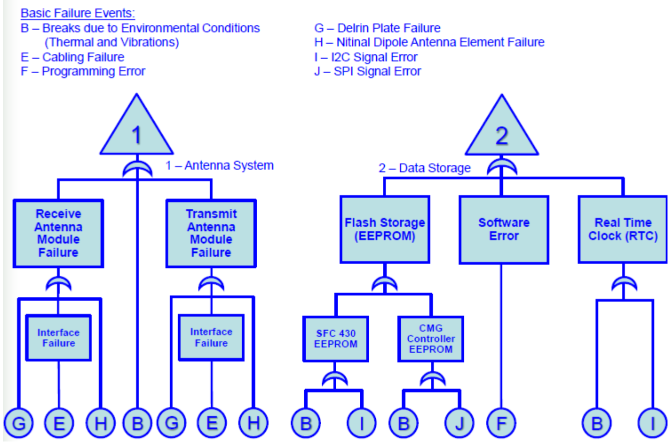


Figure 4-4. Antenna system and data storage FTA

4.2.3 EPS Subsystem FTA

As mentioned earlier, the SwampSat Electrical Power System (EPS) provides power to the entire satellite. If for any reason the SwampSat EPS fails, the EPS subsystem will not be able to provide power to other subsystems and the SwampSat mission will be a failure. The FTA for the EPS subsystem was created using the SwampSat mission and also the EPS subsystem FMECAs. The FMECA for the EPS subsystem is shown in Appendix B-4.The FTA for the EPS subsystem is shown in Figure 4-5.

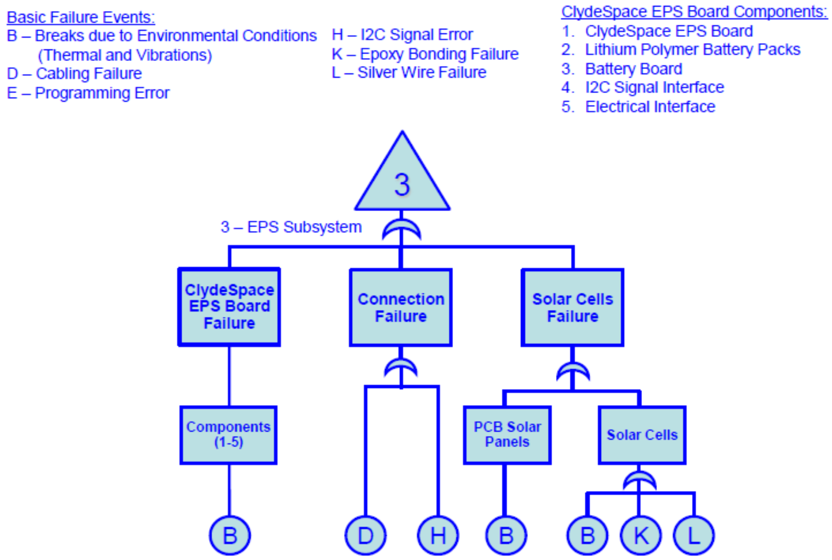


Figure 4-5. EPS subsystem FTA

The EPS subsystem failure could occur from EPS board failure, solar cell failure, or connection failure. The EPS board failure could occur from the failures of the components or software error, thus, they were represented as basic failure events. The list of the components for the EPS board can also be seen in Figure 4-5. The components could fail due to environmental conditions. The solar cells failure could occur from failures to the PCB solar panels or the solar cells itself. The PCB solar panels could fail due to environmental conditions. The solar cells could also fail due to environmental conditions. In addition the solar cells could fail if the epoxy that holds the solar cells to the PCB panels fails or if the silver wire that completes the electrical connection fails. Connection failure could occur from either cabling failure or from I2C signal error. For both possible failures, the EPS subsystem will lose communication with the other subsystems and will not be able to provide power.

From the EPS subsystem FTA, the basic failure events were identified. Environmental conditions, cabling failure, I2C signal error, epoxy bonding failure, and silver wire failure were discovered as basic failure events in the EPS subsystem FTA. In order to prevent any failures to the EPS subsystem, the basic failure events must be addressed to develop mitigation strategies.

4.2.4 CDH Subsystem FTA

The Command and Data Handling (CDH) subsystem hosts the flight computer, the SFC430, for SwampSat. If the CDH subsystem fails, SFC430 will not operate and the SwampSat mission will be unsuccessful. The FTA for the CDH subsystem was developed using the FMECAs of the CDH subsystem and the SwampSat mission. The FMECA for the CDH subsystem is shown in Appendix B-3 and the CDH subsystem FTA can be seen in Figure 4-6.

There were four lower levels identified for the CDH subsystem failure. The SFC430 failure, data storage failure, connection failure, or software error could cause the CDH subsystem to fail. The SFC430 is the main flight computer that hosts various components. The list of components on the SFC430 can be seen in Figure 4-6. The components could fail from environmental conditions, therefore basic failure event symbols were used. Another failure that could cause the SFC430 to fail was the software error.

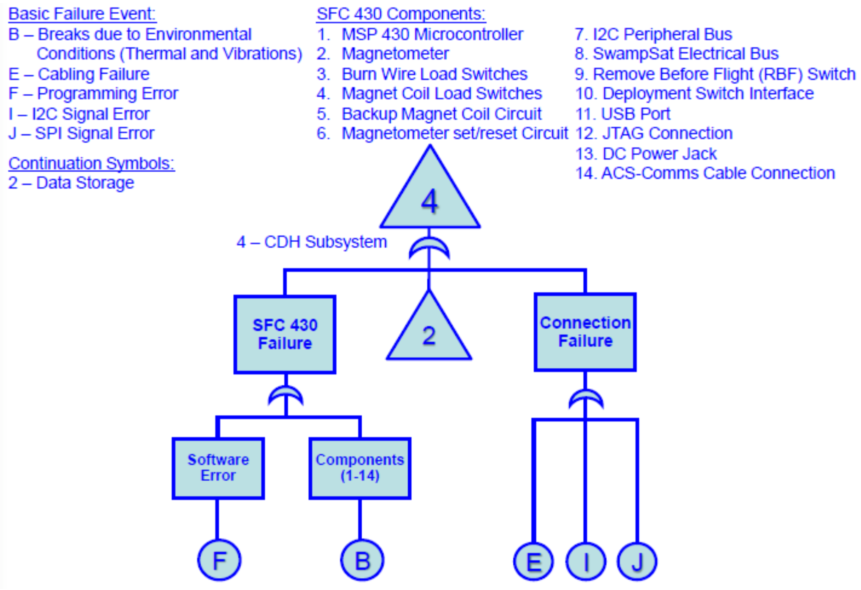

Basic Failure Event:
B – Breaks due to Environmental Conditions (Thermal and Vibrations)
E – Cabling Failure
F – Programming Error
I – I2C Signal Error
J – SPI Signal Error
Continuation Symbols:
2 – Data Storage
SFC 430 Components:
1. MSP 430 Microcontroller
2. Magnetometer
3. Burn Wire Load Switches
4. Magnet Coil Load Switches
5. Backup Magnet Coil Circuit
6. Magnetometer set/reset Circuit
7. I2C Peripheral Bus
8. SwampSat Electrical Bus
9. Remove Before Flight (RBF) Switch
10. Deployment Switch Interface
11. USB Port
12. JTAG Connection
13. DC Power Jack
14. ACS-Comms Cable Connection
4
4 – CDH Subsystem
SFC 430 Failure
2
Connection Failure
Software Error
Components (1-14)
F
B
E
I
J

Figure 4-6. CDH subsystem FTA

The SwampSat mission is operated by the SFC430 and if there were any software error, the SFC430 will not be able to execute the mission. The software error could not be expanded further, thus, it was shown as the basic failure event. The data storage is also part of the CDH subsystem and it could also cause the CDH subsystem failure. Explanation of the data storage is shown in Section 4.2.2.

Like the other FTAs, the connection failure and software error were possible reasons that the CDH subsystem would result in a failure. Connection failure could be caused by cabling failure or the I2C signal error. Programming error would cause the CDH software to fail. It was determined that the failures in the connection and in the software could not be expanded further, therefore, the basic failure symbols were used to denote the failures.

The basic failure events identified from the CDH subsystem FTA were failures due to environmental conditions, cabling failure, programming error, and I2C signal error. All of these events could fail to cause the CDH subsystem to fail. In order to prevent CDH failure, thorough plans for testing must be developed for all the basic failure events.

4.3 Safe-Hold Mode FTA

As discussed in the Chapter 3, the safe-hold mode is the primary operating mode. During the safe-hold mode, SwampSat will operate in low power mode to consume optimum power. SwampSat will remain in the safe-hold mode until commands are received from the ground station. The FTA for the safe-hold mode was constructed using the safe-hold mode FMECA shown in Table 3-6.

The safe-hold mode FTA is shown in Figure 4-7. The safe-hold mode failure could occur if battery charge fails, uplink or downlink fails, or CDH subsystem fails. Battery charge failure could occur if the EPS subsystem fails, therefore the EPS subsystem continuation symbol was used. Both the SwampSat uplink and the SwampSat downlink could fail due to several reasons, therefore the continuation symbol was denoted for both. The FTA for SwampSat uplink and SwampSat downlink can be seen in Figure 4-8. If connection failure occurs, there will be no communication between interfaces. The only cause of the connection failure was the cabling failure. If there was a software error in the safe-hold mode algorithm, the SwampSat mission will be a failure since no operations will be executed.

The basic failure events were discovered from the safe-hold mode FTA. The basic failure events identified for the safe-hold mode were cabling failure and programming error. The basic failure events of the continuation symbols can be seen in their respective FTA. Using the basic failure events, necessary actions must be taken to prevent any possible failures to the safe-hold operating mode.

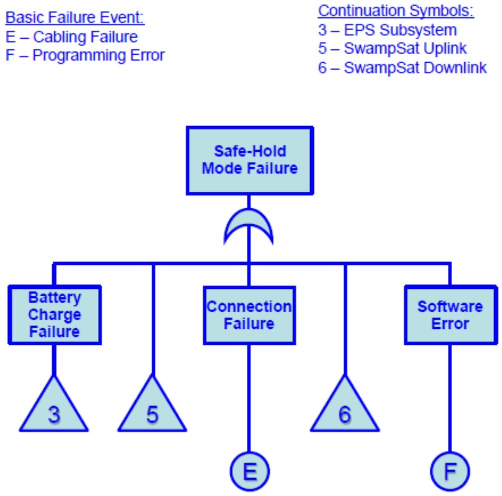


Figure 4-7. Safe-Hold mode FTA

4.3.1 SwampSat Uplink

The SwampSat uplink is established when the ground station sends commands to the SwampSat receiver. With no uplink communication established, the SwampSat mission will be a failure. The FMECA for the receiver and the ground station are shown in the TT&C subsystem FMECA located in Appendix B-5.

As shown in Figure 4-8, the SwampSat uplink failure could occur from either the receiver or the ground station components. The receiver was expanded further to determine that the failure could be caused by either the antenna system failure or the components failure on the transceiver board. The antenna system FTA was described in Section 4.2.1 and the FTA was shown in Figure 4-4. The components on the transceiver board include, receive and transmit antenna module, I2C signal interface, and electrical interface. The components could fail due to environmental conditions. The ground station components include antenna element, antenna rotor, rotor computer controller, transceiver, and terminal node controller (TNC). The components could fail due to environmental conditions as well.

4.3.2 SwampSat Downlink

The SwampSat downlink is established when SwampSat transmits telemetry from the transmitter down to the ground station. Also, during safe-hold, detumble, Comms, and ADS operating modes, the SwampSat health data will be gathered by a function, query beacon, and transmitted to the ground station. If the SwampSat downlink fails, the SwampSat mission will be unsuccessful. The details of the transmitter and the ground station were obtained from Appendix B-5, and the details of the query beacon function were acquired from the CDH subsystem FMECA located in Appendix B-3.

As discussed, the SwampSat downlink could fail if the transmitter or ground station or the query beacon function fails. The transmitter was examined deeper to find that the antenna system and the transceiver board components could fail. The transceiver components could fail due to environmental conditions. The function query beacon is a complex function, thus, the continuation symbol was denoted. Like the SwampSat uplink, the ground station components could fail from environmental conditions.

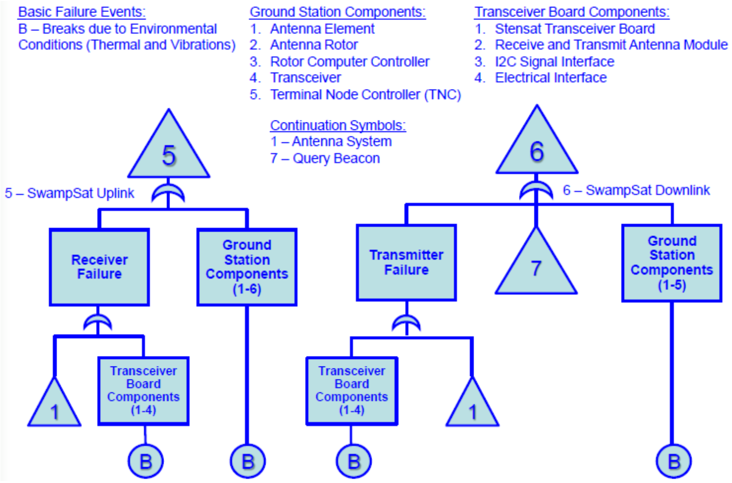

Basic Failure Events:
B – Breaks due to Environmental Conditions (Thermal and Vibrations)
Ground Station Components:
1. Antenna Element
2. Antenna Rotor
3. Rotor Computer Controller
4. Transceiver
5. Terminal Node Controller (TNC)
Transceiver Board Components:
1. Stensat Transceiver Board
2. Receive and Transmit Antenna Module
3. I2C Signal Interface
4. Electrical Interface
Continuation Symbols:
1 – Antenna System
7 – Query Beacon
5
5 – SwampSat Uplink
6
6 – SwampSat Downlink
Receiver Failure
Ground Station Components (1-6)
Transmitter Failure
7
Ground Station Components (1-5)
1
Transceiver Board Components (1-4)
Transceiver Board Components (1-4)
1
B
B
B
B

Figure 4-8. SwampSat uplink and SwampSat downlink FTA

4.3.3 Query Beacon FTA

The query beacon function is designed to read data from the CMG controller, the EPS board, the transceiver board, the ADC on SFC430, the RTC, and the EEPROM. If the function fails, the ground station will not know the real-time health of SwampSat. Not knowing the health, ground control will have a hard time deciding which commands to send to SwampSat. The FTA for the query beacon function is shown in Figure 4-9.

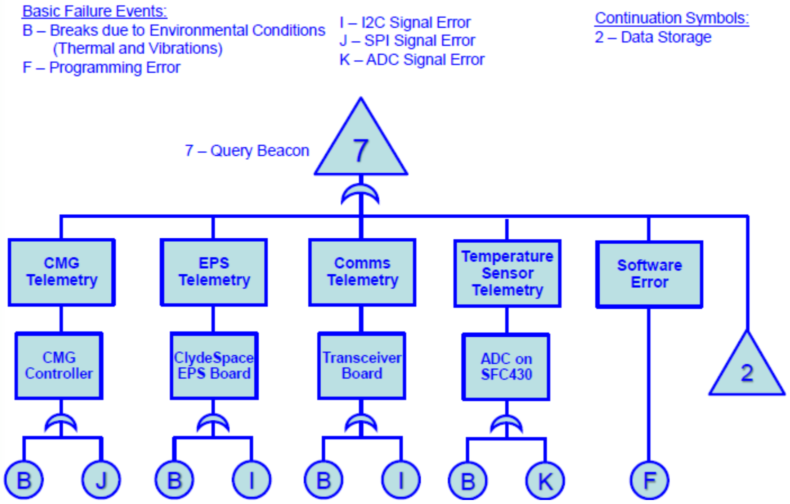


Figure 4-9. Query beacon function FTA

The query beacon function could fail if the telemetries of CMG, EPS, Comms, RTC, EEPROM, or temperature sensors fail. The RTC and the EEPROM were displayed as the data storage continuation symbol. The CMG telemetry failure occurs when the CMG controller fails. The CMG controller could fail due to environmental conditions or SPI signal error. The SFC430 communicates with the CMG controller via SPI, so, when communication is lost, SPI signal error would have occurred. The EPS telemetry failure could be caused by the failure of the EPS board. The EPS board could fail due to environmental conditions or from I2C signal error. The Comms telemetry failure could be caused by the transceiver board. The SFC430 will read the transmitter and the receiver currents from the transceiver board. The transceiver board could fail due to environmental conditions or from I2C signal error. The SFC430 communicates with the transceiver board and the EPS board through I2C, so I2C signal error results in no telemetry from the transceiver and the EPS board. The temperature sensor telemetry could fail if the ADC or the temperature sensor on the SFC430 fails. The ADC will read the temperature of the SFC430 and communicate the reading to the SFC430. The ADC on the SFC430 could fail due to environmental conditions or ADC signal error. The temperature sensor was not incorporated in the FTA since the severity of the temperature sensor failure was ranked as no impact (LS1). However, if the ADC fails, the Sun sensor readings will not be converted to be used in operations, therefore, only the ADC was shown in the FTA. The SFC430 will not be able to gather all the telemetry data if software errors occur. The query beacon is a function in the program, so if any software error occurs, the function will be rendered useless.

The basic failure events identified for the query beacon function were, environmental conditions, different signal errors, and programming error. The query beacon function is a complex function, therefore, suitable mitigation plans must be created to prevent these basic failures from happening.

4.4 Detumble Mode FTA

SwampSat will enter detumble mode when it receives commands from the ground station. During the detumble mode, the magnet coils will be powered to generate a magnetic field. The magnetic field generated for SwampSat will interact with the Earth’s magnetic field to stabilize SwampSat. If SwampSat is unable to detumble, SwampSat will not be able to perform any attitude maneuvers. The IMU will provide angular rates and they will be stored on the EEPROM. In the detumble mode, SwampSat will downlink the real-time health data to the ground. Using the detumble mode FMECA, shown in Table 3-7, the FTA for the detumble mode was developed. Figure 4-10 shows the detumble mode FTA.

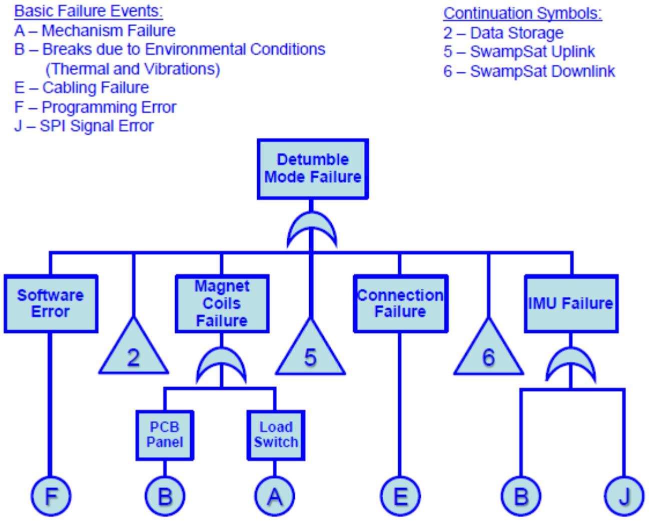


Figure 4-10. Detumble mode FTA

The detumble mode failure could occur if the magnet coils, IMU, data storage, SwampSat uplink, or SwampSat downlink fails. Also, connection failure or software error could also arise to cause unsuccessful detumble. The magnet coil failure was expanded to discover that the PCB panels or the load switch could cause the magnet coil failure. The PCB panels could break due to environmental conditions. The load switch is an electrical switch and the switch could fail from mechanism failure. When the PCB breaks, the magnet coils will not generate any magnetic field, since the magnet coils are embedded in the PCB solar panels. The load switch allows current to pass through the magnet coils to generate magnetic field. If the switch mechanism fails, SwampSat will be unable to detumble. The IMU failure could fail due to environmental conditions or SPI signal error. The IMU rates are obtained via SPI signal, therefore, no angular rates will be acquired if SPI signal error occurs. All the detumble data will be recorded on the EEPROM. The EEPROM failure was denoted as the data storage failure, shown as the continuation symbol. The SwampSat uplink and SwampSat downlink failure could occur to cause detumble failure. The FTA for the uplink and the downlink were shown in Figure 4-8. Just like the other FTAs, the connection failure or software error would result in detumble mode failure. Cabling error could result in no communication between interfaces. Programming error will cause software error for the detumble mode. With software error in the detumble mode algorithm, the SFC430 will not be able to execute the operation.

The basic failure events discovered in the detumble mode were mechanism failure, failure due to environmental conditions, cabling failure, programming error, and SPI signal error. From this, necessary arrangements and well planned testing procedures must be made to prevent detumble mode failure.

4.5 Comms Mode FTA

The Comms operating mode is designed to downlink the telemetry data from other operations to the ground station. The detumble telemetry data will be stored on the SFC430 EEPROM and the Attitude Determination System (ADS) and control moment gyroscope operations (CMG Ops) telemetry data will be kept on the CMG controller EEPROM. The ground station will command SwampSat to enter the Comms mode. In the command, the ground station can specify which telemetry data to be transmitted down. Also during Comms mode, the real-time SwampSat health data will be transmitted. The Comms mode FTA was constructed using the FMECA of the Comms mode, shown in Table 3-8. Figure 4-11 shows the FTA for Comms mode.

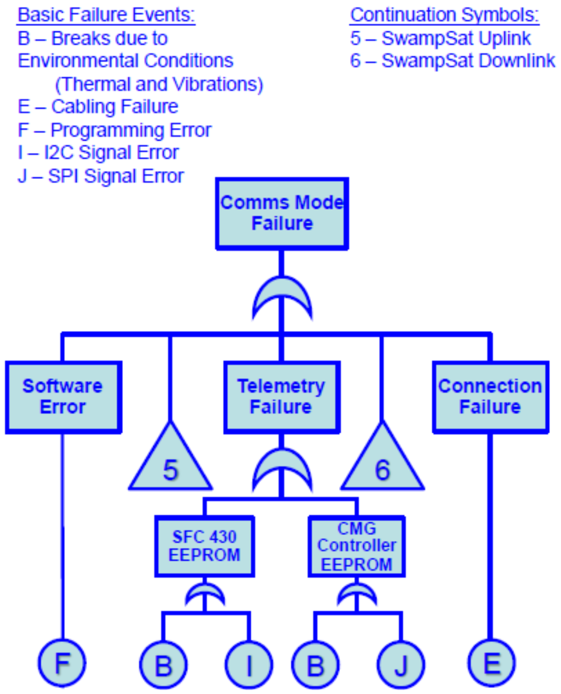


Figure 4-11. Comms mode FTA

The Comms mode could fail when uplink failure, downlink failure, failure to access telemetry, or connection failure occurs. The SwampSat uplink and SwampSat downlink failures were denoted as continuation symbols since numerous failures could cause each communication failures to occur. The FTAs for SwampSat uplink and SwampSat downlink were presented in Section 4.3.1 and Section 4.3.2. Failure to access telemetry could occur if the EEPROMs fail. As mentioned, there are two EEPROM devices, one on the SFC430 and the other on the CMG controller. Both EEPROM devices could be expanded further. The EEPROM on the SFC430 could fail if malfunction due to environmental conditions or I2C signal error occurs. Similarly, the EEPROM on the CMG controller could fail if malfunction due to environmental conditions or SPI signal error occurs. Connection failure or software error could take place to cause the Comms mode to fail. Again, the connection failure could occur from cabling failure and the software error could happen due to programming error.

The basic level failures that were determined in the Comms mode were environmental conditions, I2C signal error, SPI signal error, cabling failure, and programming error. Mitigation plans and preventative actions must be taken to avoid these basic failures from occurring during the Comms mode.

4.6 ADS Mode FTA

The ADS mode is designed to validate the ADS subsystem. The operation will begin when SwampSat receives commands from the ground station. The attitude determination and attitude estimation algorithms are both hosted on the CMG controller. The SFC430 will command the CMG controller to execute the algorithms. During execution of the algorithms, the CMG controller will request body vector measurements from the SFC430. The SFC430 will acquire Sun sensor and magnetometer measurements and proceed to compute the Sun vector and magnetic field vector. The computed data will be sent back to the CMG controller for attitude determination. The CMG controller will then read IMU rates and proceed to attitude propagation. As shown in the FMECA for the ADS operating mode, the process was denoted as attitude data. All the telemetry will be stored on the CMG controller EEPROM. Like the other operating modes, the ADS mode is also designed to transmit real-time SwampSat health data during the operation. The FTA for ADS mode is shown in Figure 4-12.

The ADS mode failure could be caused by data storage failure, uplink failure, downlink failure, attitude data failure, connection failure, or software error. Data storage, SwampSat uplink, and SwampSat downlink were all denoted as continuation symbols in the ADS mode FTA. The explanations were detailed in previous sections. The attitude data failure was also showed as a continuation symbol since various failures were identified. Figure 4-13 shows the attitude data FTA.

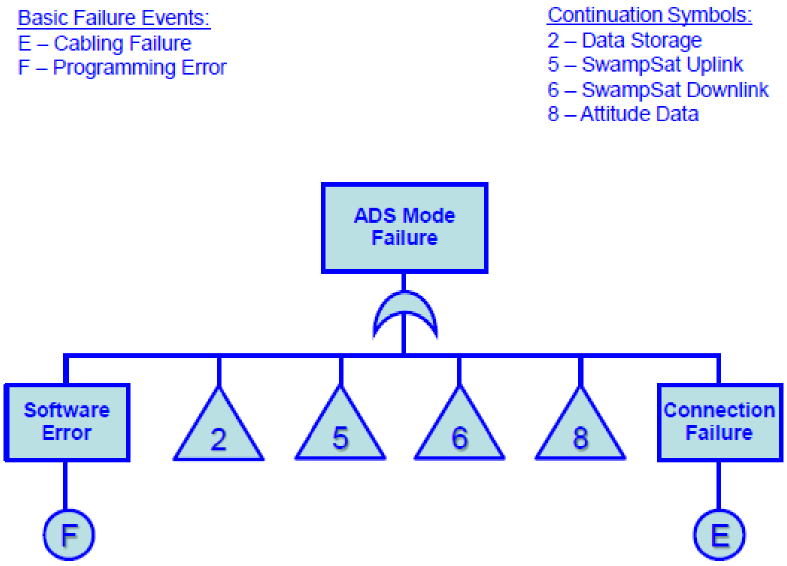


Figure 4-12. ADS mode FTA

Any connection failure or software error could cause the ADS mode to fail. Cabling issues will cause connection failure and error in the programming will result in the software error. One of the objectives for the SwampSat mission is to validate the ADS subsystem. If any of the failures shown in the ADS mode FTA occur, the ADS validation will be unsuccessful.

4.7 Attitude Data FTA

The attitude data FTA is shown in Figure 4-13. As mentioned, the attitude data includes the attitude determination and attitude propagation processes. The attitude data failure could occur from Sun sensor failure, magnetometer failure, ADC failure, IMU failure, or CMG controller failure. The Sun sensor could fail due to burn out or saturation. The Sun sensor could burn out by radiation damages and the Sun sensor saturation could occur from filter failure. Environmental conditions or burn out could cause the magnetometer to fail. Due to a power bus spike, the magnetometer could burn out. Both the Sun sensor and the magnetometer analog signals are converted into digital using the ADCs. If the ADCs fail, neither the Sun vector nor the magnetic field vector will be computed and the attitude determination will be unsuccessful. Two possible failures were identified that could cause the ADCs to fail. One possibility is the ADC could break from environmental conditions. The other possibility was the ADC signal error. If ADC signal error occurs, no analog Sun sensor signals will be converted to digital signals, thus, resulting in no attitude determination and no validation of ADS subsystem. The I2C signal error was another possibility that could cause the ADC failure. The I2C communication link is established between the SFC430 and AD7994. If I2C signal error occurs, the magnetic field vector will not be computed and will lead to attitude determination failure. The angular rates from the IMU will be used in the attitude propagation algorithm. The IMU could fail from either environmental conditions or from SPI signal error. The CMG controller reads the IMU rates through SPI communication link. As mentioned, the CMG controller hosts the algorithms to operate the validation of the ADS subsystem. CMG controller failure not only could cause ADS mode failure, but also the SwampSat mission failure too. The CMG controller failure occurs if the software or the components fail. The list of the components is also shown in Figure 4-13. The software error could be caused by programming error. The components on the CMG controller could fail due to environmental conditions.

The basic failure events identified for the attitude data failure were failures due to environmental conditions, programming, I2C signals, SPI signals, ADC signals, Sun sensor filter, radiation damage, and power bus spike. Any of the basic failures events will cause the attitude data failure. To avoid the attitude data failure, the basic failure events must be looked into carefully to come up with testing procedures.

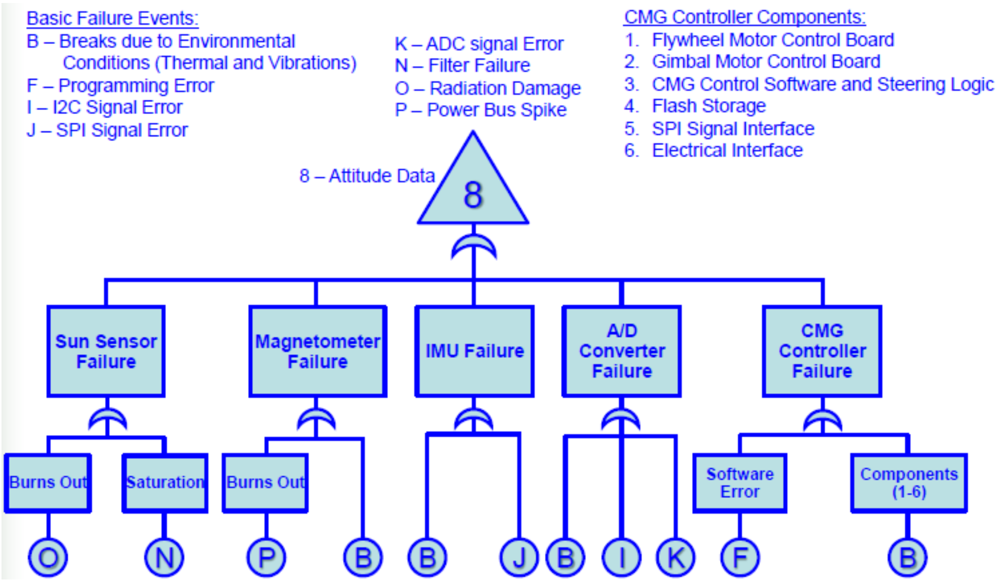


Figure 4-13. Attitude data FTA

4.8 CMG Ops Mode FTA

The CMG Ops mode is designed to validate the ACS subsystem of SwampSat. During the CMG Ops mode, SwampSat will perform CMG maneuvers to validate rapid retargeting and precision pointing (R2P2). The CMG Ops mode is the most power intensive operation, therefore transmission to the ground station is omitted. Like the ADS mode, the CMG Ops mode will request attitude data. Using the attitude determined in the ADS mode, the attitude maneuvers can be performed using the CMGs. The FTA for the CMG Ops mode was developed using the FMECAs of the CMG Ops mode and the ACS subsystem. The CMG Ops FTA is shown in Figure 4-14.

Looking at the CMG Ops FTA, the failure for the mode could occur from data storage failure, SwampSat uplink failure, attitude data failure, CMG failure, connection failure, or software error. The CMG Ops mode has similar functionality as the ADS operating mode.

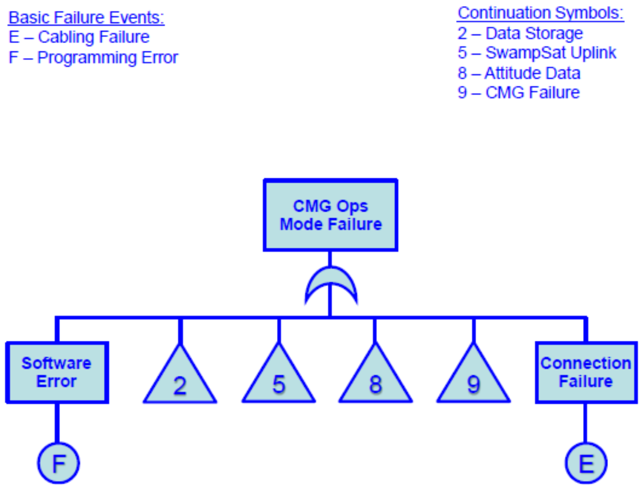


Figure 4-14. CMG Ops mode FTA

The difference between the CMG Ops FTA and the FTA for the ADS mode was that the CMG failure was added for the CMG Ops mode FTA. Also, since the transmitter is completely turned off, the SwampSat downlink failure was removed from the Father continuation symbols were used for the data storage, SwampSat uplink, attitude data, and the CMG failures. Detailed explanation of the CMG FTA is shown in the next section and the FTA is shown in Figure 4-15. Just like the other FTAs, the connection failure could occur due to cabling failure and programming error will cause the software to fail.

4.9 Control Moment Gyroscope FTA

From the FTA for the CMG, the following failures were identified that could cause the CMG failure; flywheel failure, gimbal failure, CMG controller board failure, software error, and pyramid configuration failure. The flywheel failure could occur from environmental conditions, bearing contamination, flywheel motor failure, slip ring failure, cold welding, bracket failure, or fasteners failure. The gimbal failure could occur from similar failures as the flywheel failures.

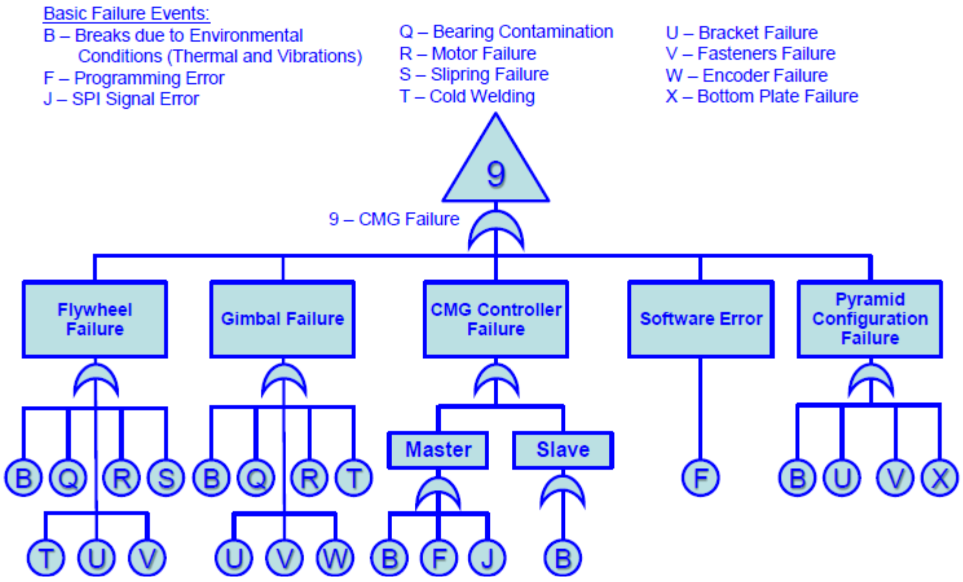


Figure 4-15. Control moment gyroscope FTA

The gimbal failure could occur from environmental conditions, bearing contamination, gimbal motor failure, cold welding, bracket failure, fasteners failure, or encoder failure. The motor driver board failure could occur to cause the CMG to fail. The CMG controller is located on the motor driver board. There are two separate boards, one is the master and the other is the slave. Both motor driver boards could fail due to environmental conditions or by programming error. Additionally the master motor driver board communicates to the SFC430 via SPI communication, therefore the SPI signal error was included in the FTA. The software error could occur due to programming error. Four CMGs will be assembled in a pyramid configuration for the SwampSat mission. The pyramid configuration failure could occur when the configuration breaks due to environmental conditions or when the brackets that hold the configuration together fails, or when the fasteners loosens, or when the bottom plate that the CMGs rest on breaks.

The basic failure events that were identified from the FTA for the CMG were environmental conditions, programming error, SPI signal error, bearing contamination, flywheel or gimbal motor failure, slip ring failure, cold welding, bracket failure, fasteners failure, encoder failure, and the bottom plate failure. Using the basic failure events from the FTA, the CMG failures could be avoided by developing efficient methods of testing. Not only testing, thorough analysis must be conducted to eliminate any possible failures of the CMG. The CMGs are the heart of SwampSat, therefore, any possible failures must be eliminated.

4.10 Summary

The SwampSat FTA was constructed using the most severe failure modes from the SwampSat FMECA. The most severe failure modes from the SwampSat FMECA were analyzed further to identify the root causes for those failures. The lowest level failures were represented as the basic failure events. The basic failure events for each operating modes and subsystems and their potential mitigation plans are described here. As previously stated, the focus of the reliability analysis was the SwampSat operating modes, therefore, the basic failure events for the launch stage will not be discussed.

The following basic failure events were identified in the deployment/startup stage; mechanism failure, environmental conditions, dead battery, cabling failure, and programming error. The antenna system, data storage, EPS subsystem, and the CDH subsystem were identified as complex systems, therefore, the continuation symbols were assigned. The mechanism failure was the root cause of the deployment spring failure, P-POD door failure, burn wire failure, load switch failure, premature antenna deployment, and separation switch failure. As previously mentioned the P-POD is the Cal Poly’s responsibility, therefore, the SwampSat team will have no control. The burn wire mechanism can be prevented by performing functionality test on the antenna deployment system to ensure successful antenna deployment. In addition, the load switch and the separation switch can be tested for its functionality. Environmental testing, vibration and thermal testing, can be performed on the antenna system to prevent any possible premature antenna deployment. The battery must be carefully tested by charging and discharging and also the battery must be stored properly to avoid any damage. As stated in the SwampSat FMECA, each connection will be tested for its functionality and a layer of epoxy can be added to ensure no connections become loose. Also, the software for the deployment/startup stage can be carefully debugged and simulated to ensure the algorithm has no programming error.

From the antenna system FTA, the following basic failure events were identified as the root causes; failure due to environmental conditions, cabling failure, delrin plate failure, nitinol dipole antenna element failure. Environmental testing can be performed to prevent failures due to environmental conditions. The cabling can be tested by checking each connection and applying epoxy to secure the connections. The delrin plate and the antenna element can also be tested in environmental conditions to ensure no potential failure would occur.

The data storage FTA showed these basic failure events as the root causes; failure due to environmental conditions, programming error, I2C signal error, and SPI signal error. Environmental conditions can cause the two EEPROM devices and the RTC to fail. Environmental testing can be performed to mitigate any potential failures caused by environmental conditions. All the software for the EEPROM and the RTC can be debugged and simulated to ensure no programming error will occur. Communication testing can be performed to prevent any I2C or SPI signal errors to occur.

The following basic failure events were identified from the EPS subsystem FTA; failure due to environmental conditions, cabling failure, programming error, I2C signal error, epoxy bonding failure, and silver wire failure. For the failure due to environmental conditions, the EPS board and the PCB solar panels with solar cells can be put through environmental testing, vibration and thermal testing, to avoid any potential failure by environmental conditions. The cabling can be tested between interfaces to ensure power is provided by the EPS. All the software for the EPS subsystem can be debugged and simulated to ensure no programming error will occur. Once the solar cells are mounted on the PCB solar panels, the panels can be placed on the vibration shaker table to ensure the solar cells do not get loose. Also, once the solar cells are mounted, functionality tests can be performed on the solar cells to ensure there is electrical connection between the solar cells and the solar panels.

From the CDH subsystem FTA, the following basic failure events were identified; failure due to environmental conditions, cabling failure, programming failure, and I2C signal error. The SFC430 board can be tested using the vibration shaker table and the thermal vacuum chamber to mitigate any potential failure due to environmental conditions. The cabling can be tested by checking and adding a layer of epoxy to each connection to ensure secure connection between interfaces. Programming error must be avoided, therefore, careful debugging and simulation must be performed to ensure no software failure. In addition, the I2C signal can be tested by running sample codes to ensure there is communication. The data storage is part of the CDH subsystem, therefore, the continuation symbol was used.

The following basic failure events were identified for the safe-hold mode; cabling failure and programming error. The continuation symbols were used for EPS subsystem, SwampSat uplink, and SwampSat downlink since they were complex systems. Each connection can be tested and a layer of epoxy could be added to prevent the connections from getting loose. By simulating and debugging the code, potential programming error can be avoided. Since the safe-hold mode is the main operating mode for SwampSat, special attention must be need when simulating and debugging the software.

From the SwampSat uplink FTA, the failure due to environmental conditions was the basic failure event that was identified. However, the antenna system failure could also occur, therefore, the continuation symbol was denoted for the antenna system. Also, for the SwampSat downlink FTA, the failure due to environmental conditions was the basic failure event and the antenna system was represented as the continuation symbol. Query beacon was also represented as a continuation symbol since it can be expanded further to identify the potential lower level causes of failure. The transceiver can be put through environmental testing to prevent any potential failure due to environmental conditions. The ground station equipment can be checked regularly and can be replaced if necessary.

The query beacon FTA identified the following root causes; failure due to environmental conditions, programming error, I2C signal error, SPI signal error, ADC signal error, or programming error. As previously mentioned, the query beacon is a function that gathers the health data for SwampSat. The data will be stored on the two EEPROM devices, therefore, the data storage continuation symbol was added to the

FTA. If components fail due to environmental conditions, the function will not gather data from the CMG controller, EPS board, transceiver board, or the ADC. The I2C signal error could result in no communication between the SFC430 and the EPS board, or between the SFC430 and the transceiver board. The SPI signal error can cause the communication between the SFC430 and the CMG controller to fail. The ADC signal error can result in no communication between the SFC430 and the ADC. To prevent possible failure due to environmental conditions, each components can be put through environmental, thermal and vibration, testing and functionality testing can be performed after the environmental testing. While performing functionality testing, each signal can be tested by running software to ensure the SFC430 can communicate with each components. The query beacon function can be carefully debugged and simulated to prevent any possible programming error.

The following root causes were identified from the detumble mode FTA; mechanism failure, failure due to environmental conditions, cabling failure, programming error, and SPI signal error. The continuation symbols were represented for data storage, SwampSat uplink, and SwampSat downlink. The load switch mechanism could fail to cause the magnet coils failure. The load switch can be tested for its functionality to prevent possible failure. The PCB solar panels can fail due to environmental conditions, thus, environmental testing can be performed on the PCB solar panels to prevent possible failure. The IMU failure can be caused by environmental conditions or the SPI signal error. The IMU can be put through environmental testing and functionality tests can be performed after the environmental testing to ensure the IMU works. While testing the functionality, the SPI communication can be tested to ensure the SFC430 can read the angular rates. Each connection can be tested and a layer of epoxy can be added to prevent possible cabling failure. The algorithm for the detumble operating mode can be debugged and simulations can be performed to prevent possible programming error.

The Comms operating mode FTA identified the following potential basic failure events; failure due to environmental conditions, cabling failure, programming error, I2C signal error, and SPI signal error. The continuation symbols were used for the SwampSat uplink and the SwampSat downlink. The telemetry failure could be caused by either the SFC430 EEPROM or the CMG controller EEPROM. The SFC430 EEPROM could fail due to environmental condition or I2C signal error. The CMG controller EEPROM could fail due to environmental conditions or SPI signal error. Environmental testing can be performed for both EEPROM devices and their functionality can be tested upon completion of the environmental testing. During the functionality tests, the I2C and the SPI communication can be carefully tested to prevent any possible signal errors. As mentioned previously, each connection can be tested and a layer of epoxy can be added to prevent any potential cabling failure. The Comms mode algorithm can be thoroughly debugged and simulations can be performed to ensure there is no programming error in the software.

The basic failure events that were identified from the ADS mode FTA were cabling failure and programming error. There were four continuation symbols in the ADS FTA; data storage, SwampSat uplink, SwampSat downlink, and attitude data. Connection failure can be prevented by testing each connection and if necessary, a layer of epoxy can be added to prevent potential cabling failure. Careful debugging and running simulations can be performed to prevent any programming error in the ADS operating mode algorithm.

The attitude data FTA was constructed to represent potential basic failure events from the Sun sensors, magnetometer, IMU, ADC, and the CMG controller. The following basic failure events were identified from the attitude data FTA; failure due to environmental conditions, programming error, I2C signal error, SPI signal error, ADC signal error, filter failure, radiation damage, and power bus spike. The Sun sensors could fail if saturation occurs due to filter failure or the sensors burn out due to radiation damage. The Sun sensors can be tested for its functionality under a light source to check for any saturation and the filter can be replaced if necessary. Furthermore, the Sun sensors can be placed inside the thermal vacuum chamber for thermal testing to prevent any possible damages from radiation. The magnetometer can burn out due to a power bus spike, therefore, the magnetometer must be tested to ensure that it could withstand power spike and be replaced if necessary. The magnetometer can be put through environmental testing to prevent possible failure from environmental conditions. The IMU can also be put through environmental testing to prevent failure due to environmental conditions and while performing functionality tests, the SPI communication link can be verified to prevent any potential SPI signal error. As previously stated, there are two ADC devices on SwampSat. Both could fail due to environmental conditions, however, environmental testing can be performed to prevent potential failure. The external ADC communicates through I2C, therefore, the communication can be verified by running sample codes. The ADC on the SFC430 communicates through ADC signal, therefore, samples codes can be simulated to verify the communication. The CMG controller could fail from programming error or failure of the components due to environmental conditions. Environmental testing can be performed on the components to prevent any possible failures due to environmental conditions. The algorithms for the ADS verification process which are hosted on the CMG controller can be debugged and simulations can be performed to ensure that no programming error occurs.

From the CMG Ops mode FTA, cabling failure and programming error were identified as the basic failure events. Data storage, SwampSat uplink, attitude data, and CMG failure were denoted as continuation symbols to represent potential root causes. All the connection on SwampSat can be tested and epoxy could be added to prevent any cabling failure. Thorough debugging and simulations can be performed on the CMG Ops mode algorithm to prevent any programming error.

The CMG FTA was the most complex FTA constructed for SwampSat. The following basic failure events were identified for the CMG FTA; failure due to environmental conditions, programming error, SPI signal error, bearing contamination, motor failure, slipring failure, cold welding, bracket failure, fasteners failure, encoder failure, and bottom plate failure. To prevent any failures caused by environmental conditions, the components can be put through environmental testing. All the software can be carefully debugged and simulations can be performed to prevent any potential programming error. The CMG controller communicates with the SFC430 through SPI communication, therefore, to verify the communication, sample codes can be simulated. To prevent bearing contamination, lubricant can be applied to the bearings. Functionality tests for the flywheel motors and the gimbal motors can be performed to prevent potential failures. To prevent any cold welding, the CMGs can be placed inside the vacuum and functionality tests can be performed on the CMGs. To prevent slipring failure, bracket failure, or fasteners failure, the assembled CMGs can be put through functionality tests and the parts can be replaced if necessary. The encoder failure can be prevented by running sample codes to ensure no programming error. The bottom plate failure can be prevented by placing the bottom plate on the vibration shaker table and in the thermal vacuum chamber to undergo environmental testing.

From the SwampSat FTA, the following basic failure events were identified the most; environmental conditions, programming error, cabling failure, and mechanism failure. Priority must be addressed to the basic failure events with the most appearance and thorough mitigation plans must be developed. However, the other basic failure events must be addressed as well to develop necessary mitigation plans for those basic failure events.

CHAPTER 5
CONCLUSION AND FUTURE WORK

5.1 Conclusion

Reliability analysis was conducted on the first CubeSat developed at the University of Florida. The Space Systems Group has designed and is currently developing SwampSat, a 1U picosatellite, whose mission objective is to validate in flight a compact three-axis attitude control system using miniature control moment gyroscopes. The CMGs will perform attitude maneuvers to confirm the ability of rapid retargeting and precision pointing. Two types of reliability analyses were conducted for SwampSat. Failure, Modes, Effects, and Criticality Analysis and the Fault Tree Analysis for SwampSat were presented in this thesis. The SwampSat mission was divided into seven different stages, namely launch, deployment/startup, safe-hold mode, detumble mode, Comms mode, Attitude Determination System mode, and control moment gyroscope operations mode. For each stage, the FMECA and the FTA were conducted to examine in detail the possible failures. The SwampSat FMECA identified failure modes with high criticality. The criticality was calculated from the severity and the likelihood of the failure modes. Using the SwampSat FMECA, the FTA was developed. The SwampSat FTA provided a visible representation of the critical paths down to the lowest possible root causes.

The two analyses discovered potential failures for SwampSat. Using the high criticality items from FMECA and the basic failure events from the FTA, brief mitigation plans and preventative actions were discussed. Most components on SwampSat are built in-house, meaning they have no prior flight experience and there is no knowledge of how they will perform in orbit, therefore, those components were denoted as high severity and high likelihood of occurrence. The high criticality items were assigned for components such as the CMGs, Sun sensors, and software for each operating modes. The failure due to environmental conditions and programming error were the most common basic failure events identified in the SwampSat FTA. Individual components on SwampSat can be put through environmental testing and once SwampSat is fully integrated, SwampSat can be put through environmental testing to ensure no failure due to environmental conditions. Each software can be tested and when SwampSat is fully integrated, all the software can be tested again to ensure no programming error. Further mitigation plans must be developed by the SwampSat team. Priority will be to address the high criticality items and the basic failure events. However, the moderate and low criticality items must never be underestimated.

5.2 Future work

Brief mitigation plans for each failure were discussed in this thesis, however, these mitigation plans should be examined further. The challenge will be to determine well planned mitigation and prevention procedures for the failures. Also, the reliability analyses for SwampSat are an ongoing process. The process will continue until SwampSat gets launched.

The next step is to formalize the techniques for any generic CubeSat mission. By using the FMECA and the FTA techniques, high risks and critical paths can be identified and appropriate mitigation plans can be developed for any CubeSats. The results from the SwampSat FEMCA and the SwampSat FTA can be used as reference for future projects.

APPENDIX A
SOFTWARE ARCHITECTURE

The software architectures for the SwampSat mission are shown in this section. Figure A-1 shows the software architecture for the Safe-hold mode. Figure A-2 shows the software architecture for the functions Query Beacon and Deploy Antenna. Figure A-3 shows the software architecture for the detumble mode. Figure A-4 shows the software architecture for the functions power on magnet coils and record detumble telemetry. Figure A-5 shows the software architecture for the Comms operating mode. Figure A-6 shows the software architecture for the function access telemetry. Figure A-7 and Figure A-8 are the software architectures for the ADS and the CMG Ops mode, respectively. The software architecture has been developed as a part of the CDH subsystem. In SSG member, Sharanabasaweshwara Asundi's dissertation titled, "CubeSat System Design Based on Methodologies Adopted for Developing Wireless Robotic Platform", the software architecture is explained in detail [6].

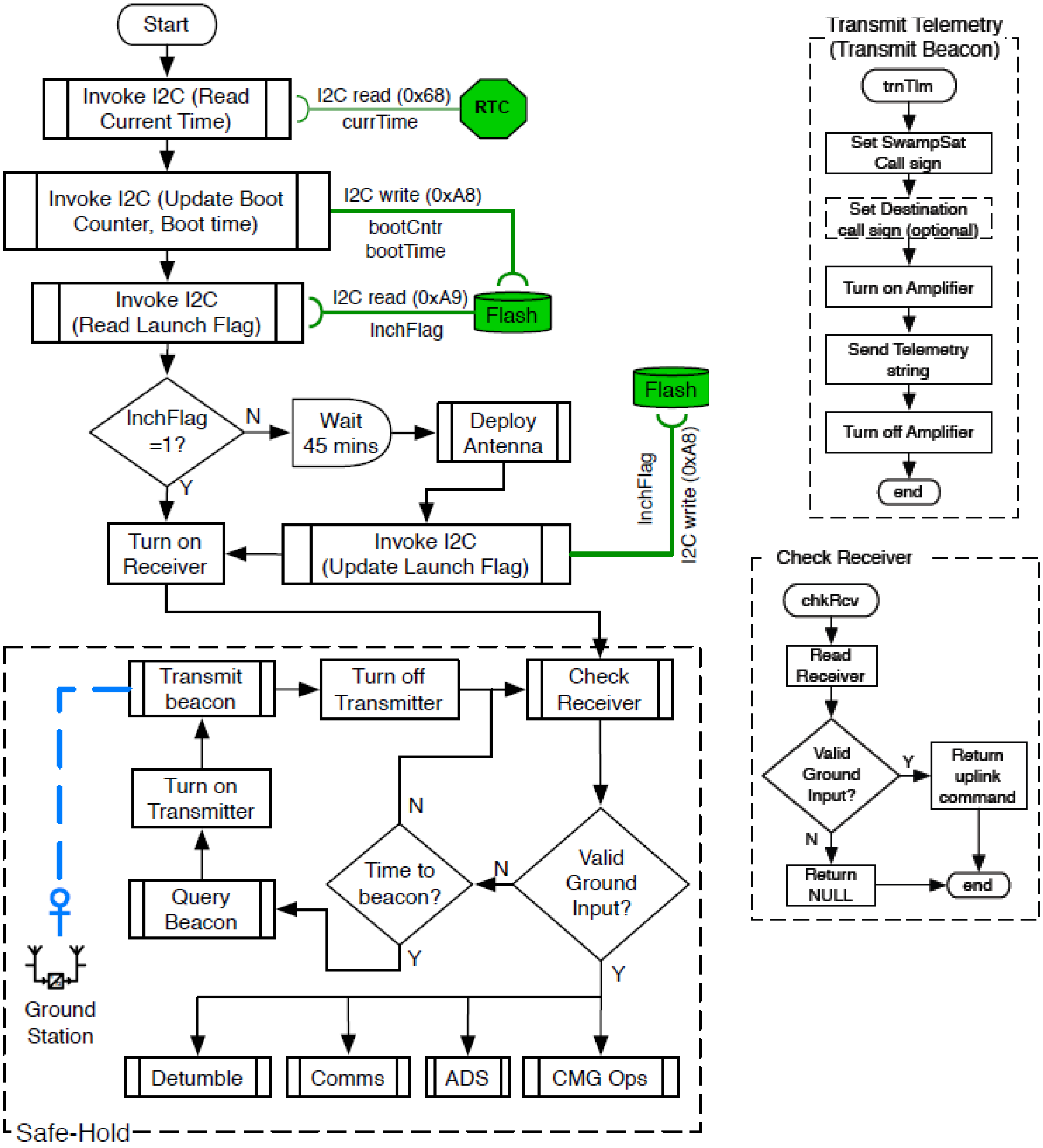


Figure A-1. Safe-Hold mode software architecture

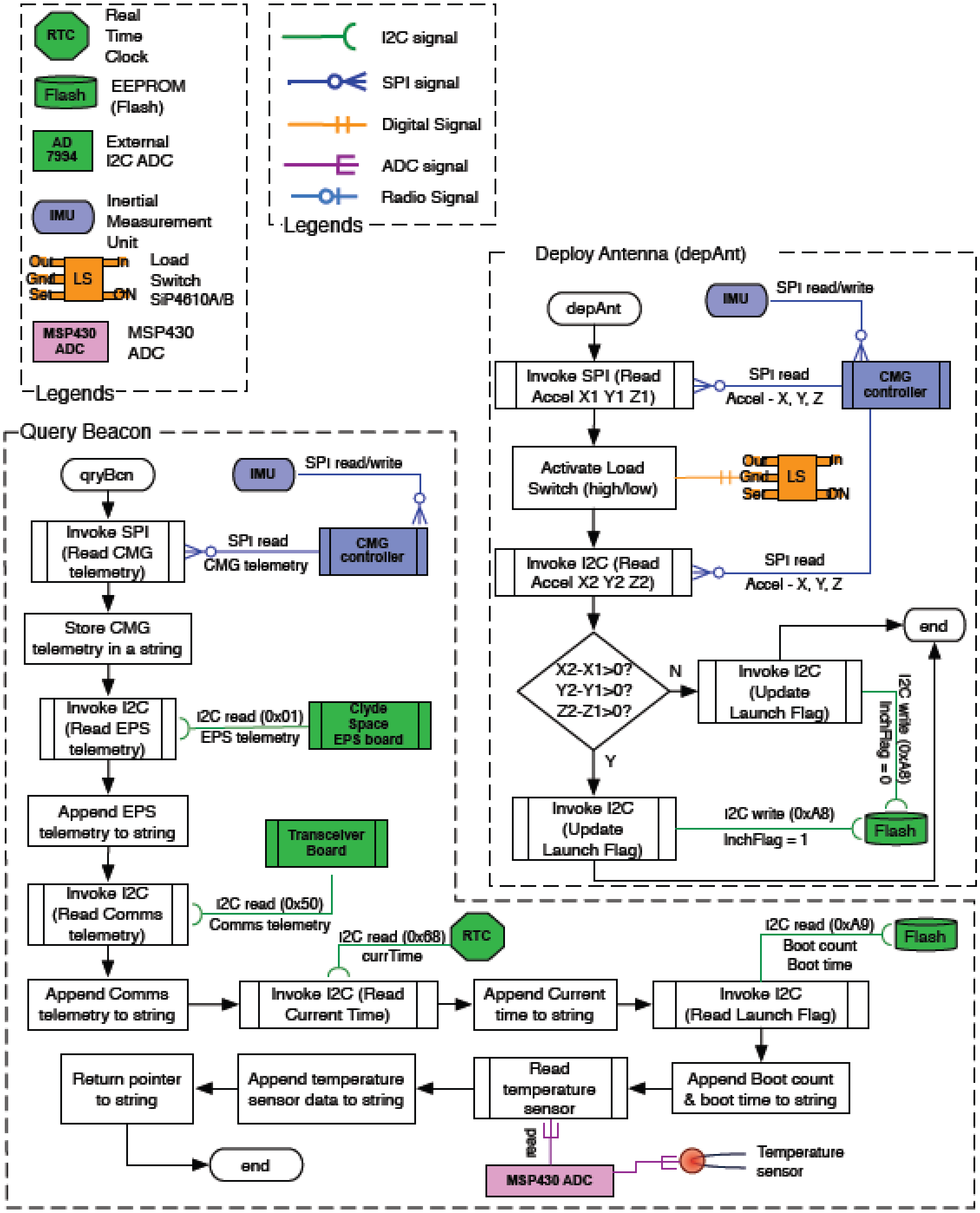


Figure A-2. Functions query beacon and deploy antenna

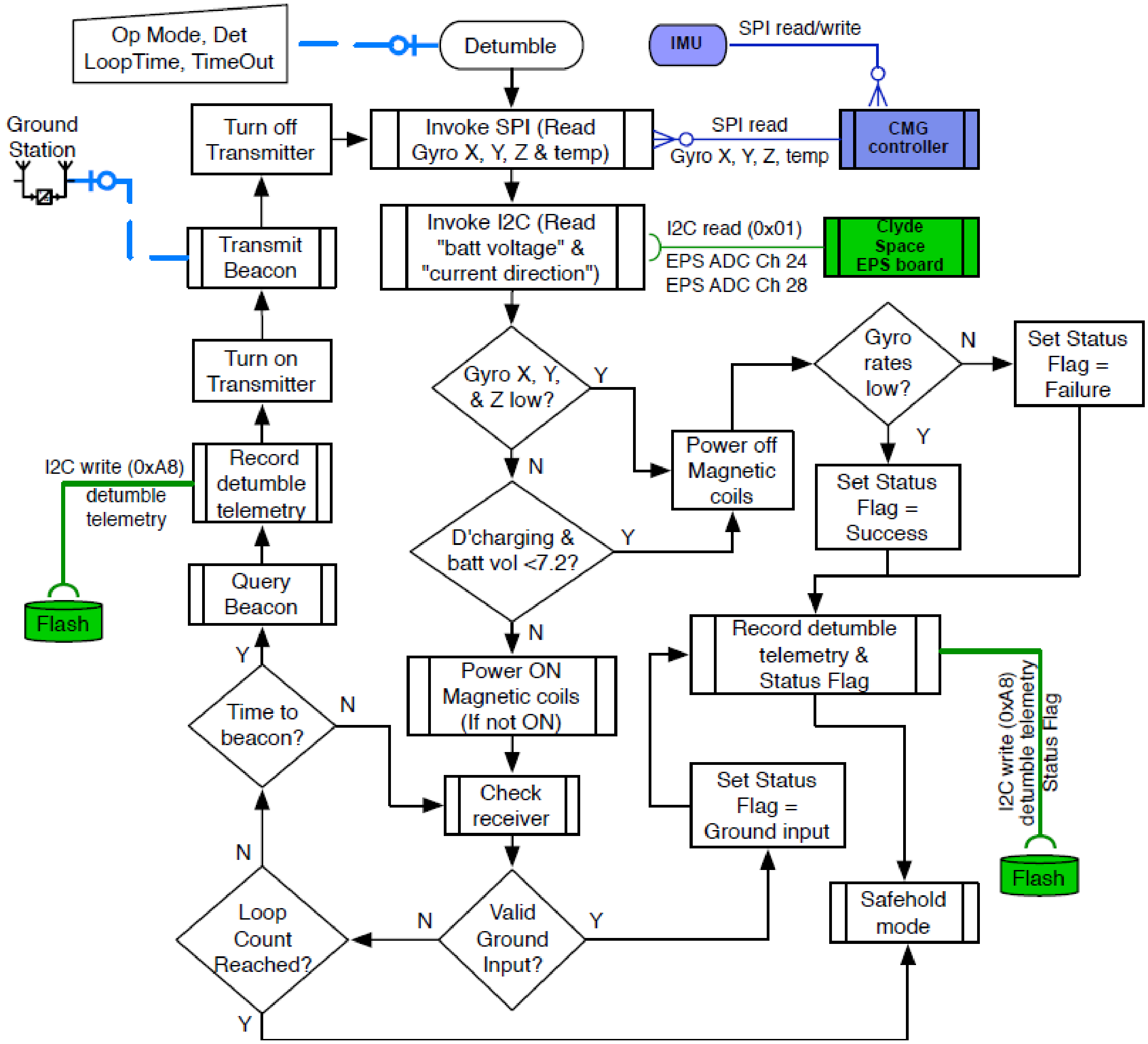


Figure A-3. Detumble mode software architecture

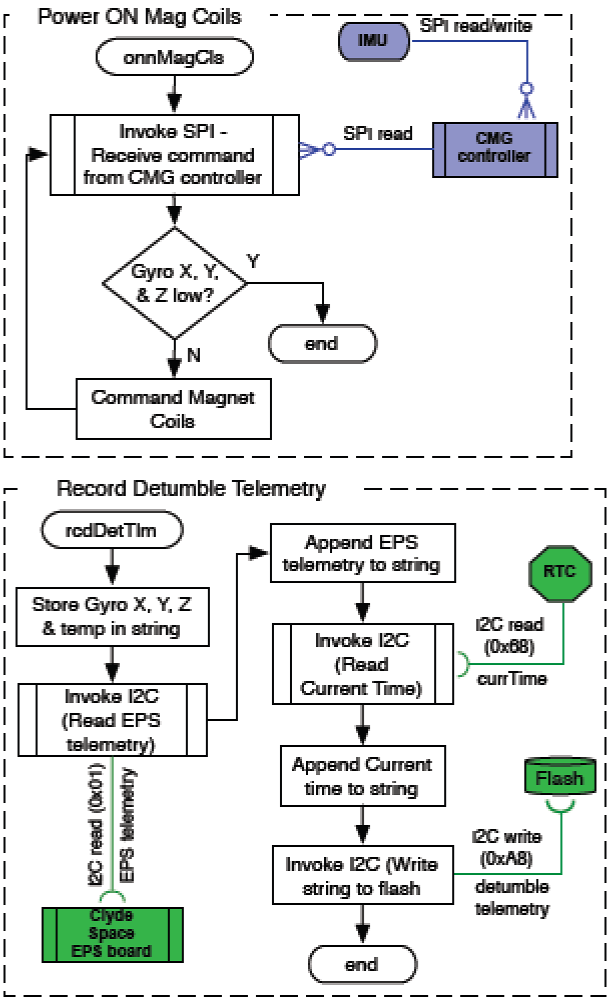

Power ON Mag Coils
onnMagCls
IMU
SPI read/write
Invoke SPI - Receive command from CMG controller
SPI read
CMG controller
Gyro X, Y, & Z low?
Y
end
N
Command Magnet Coils
Record Detumble Telemetry
rcdDetTlm
Store Gyro X, Y, Z & temp in string
Invoke I2C (Read EPS telemetry)
I2C read (0x01)
EPS telemetry
Clyde Space EPS board
Append EPS telemetry to string
RTC
Invoke I2C (Read Current Time)
I2C read (0x68)
currTime
Append Current time to string
Flash
Invoke I2C (Write string to flash
I2C write (0xA8)
detumble telemetry
end

Figure A-4. Functions power on magnet coils and record detumble telemetry

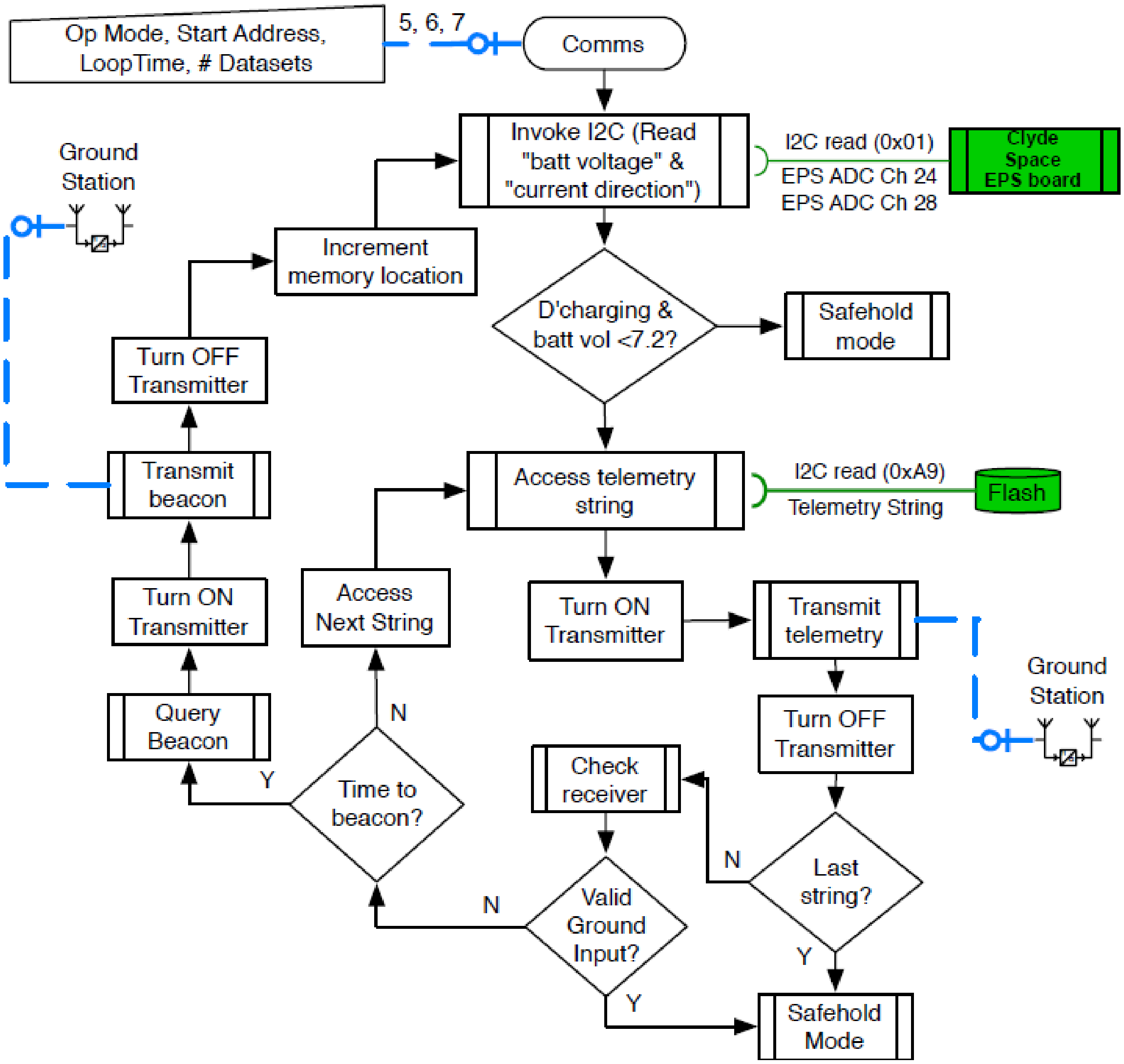


Figure A-5. Comms mode software architecture

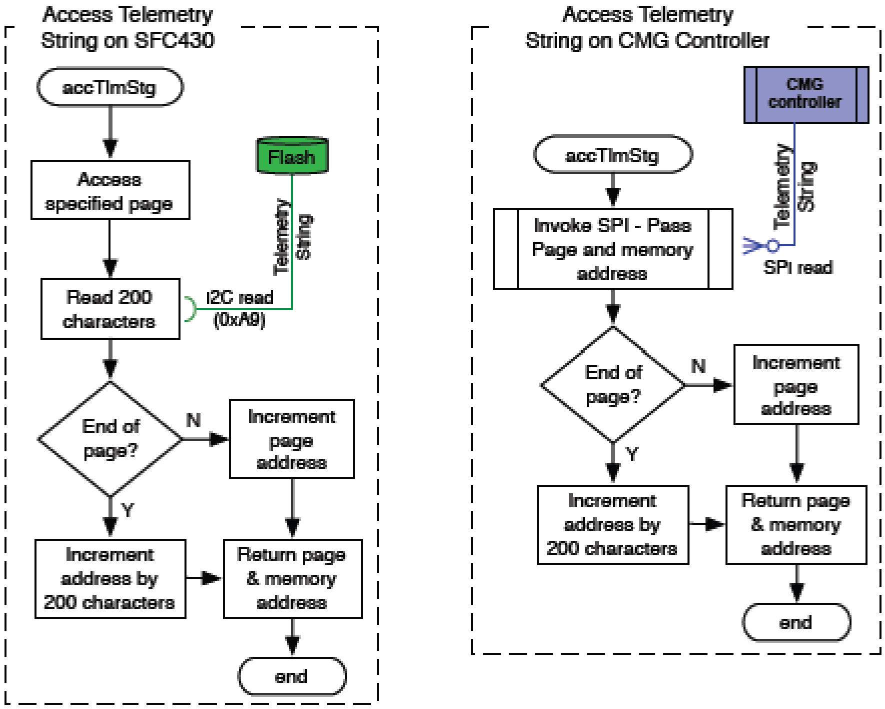

Access Telemetry String on SFC430
accTlmStg
Access specified page
Flash
Telemetry String
Read 200 characters
I2C read (0xA9)
End of page?
N
Y
Increment page address
Increment address by 200 characters
Return page & memory address
end
Access Telemetry String on CMG Controller
CMG controller
accTlmStg
Invoke SPI - Pass Page and memory address
Telemetry String
SPI read
End of page?
N
Y
Increment page address
Increment address by 200 characters
Return page & memory address
end

Figure A-6. Functions access telemetry string on SFC430 and CMG controller

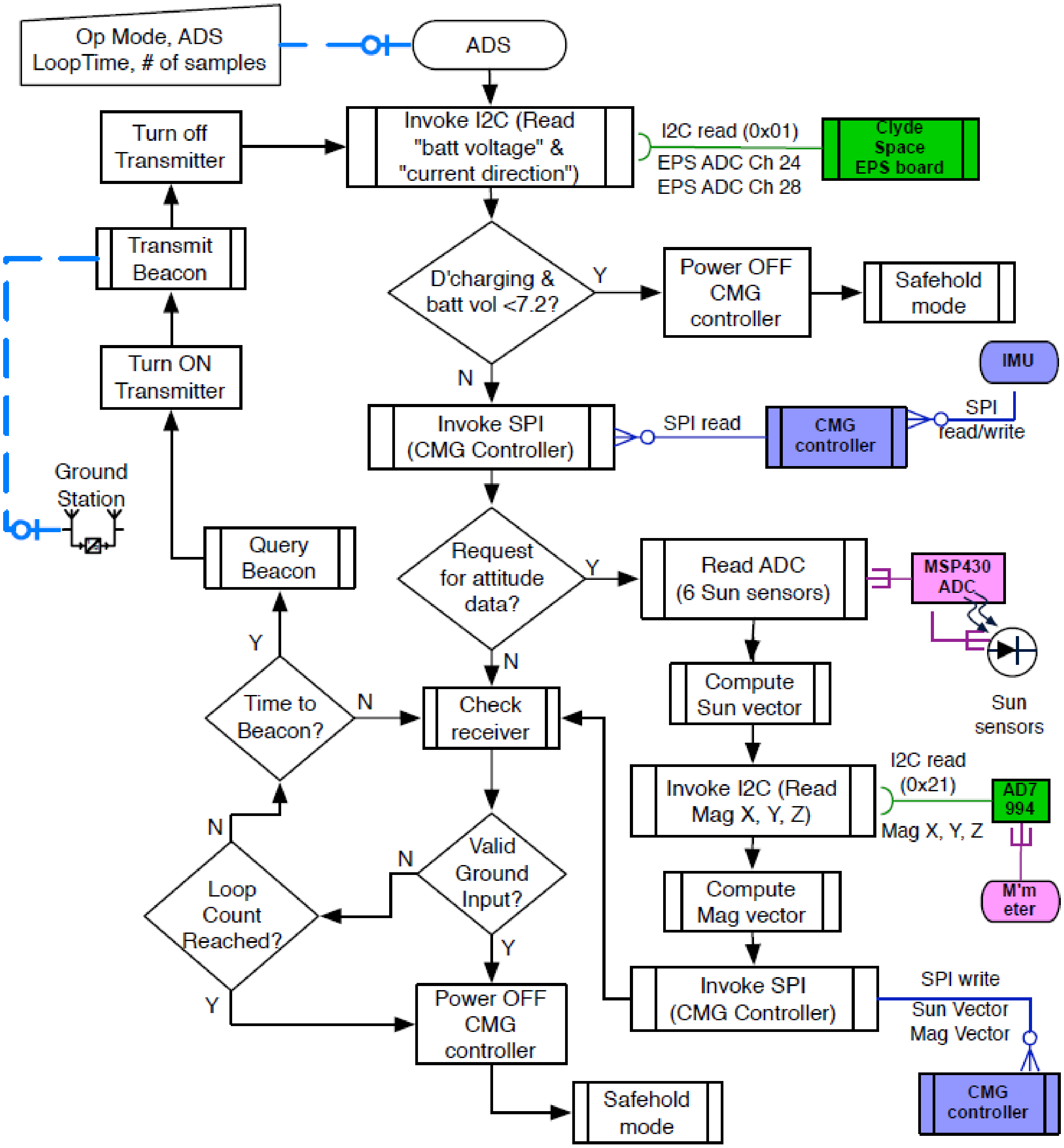


Figure A-7. ADS mode software architecture

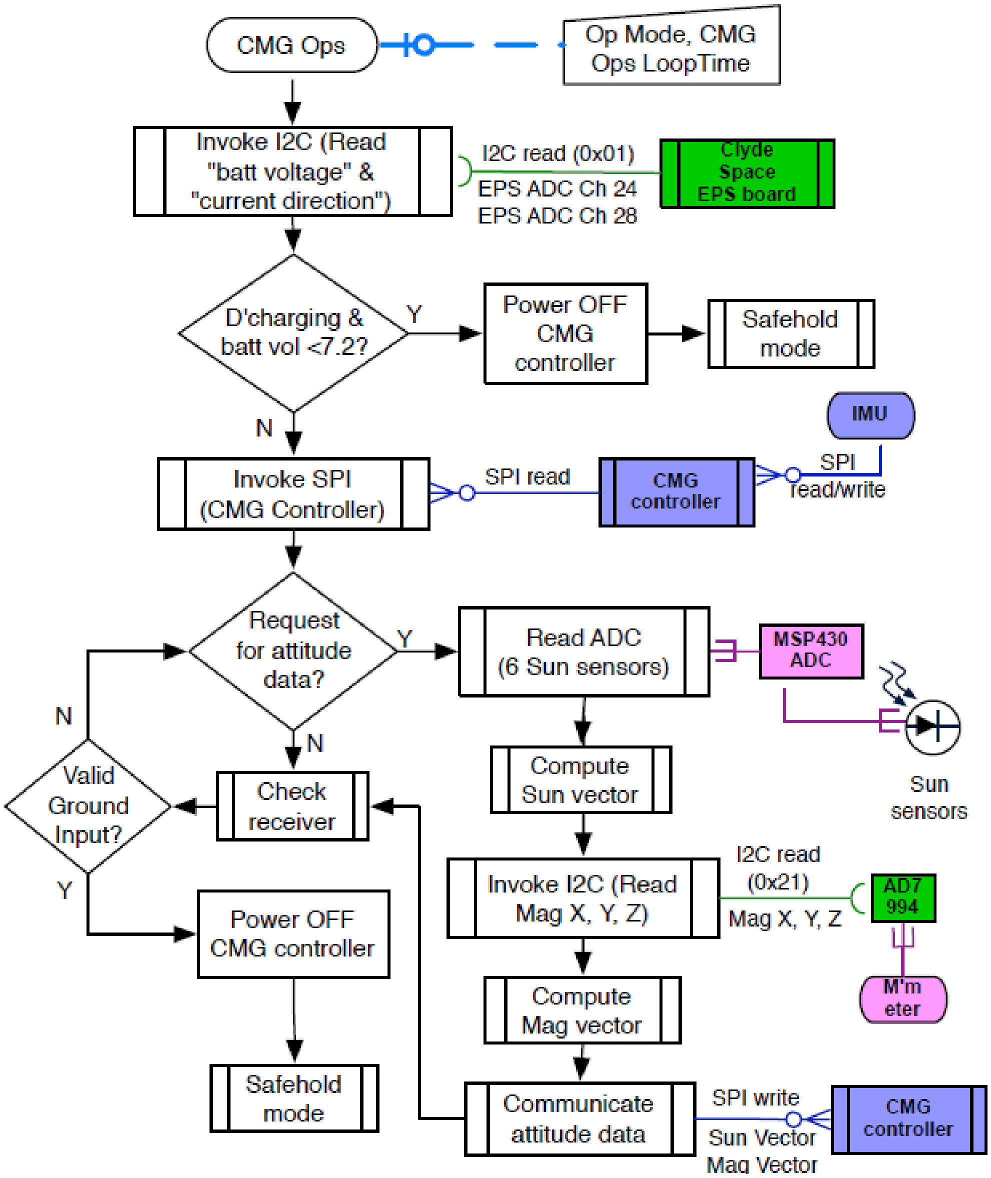


Figure A-8. CMG Ops mode software architecture

APPENDIX B
FMECA OF THE SUBSYSTEMS

The FMECA for the SwampSat mission did not cover in detail of each of the failure modes. In this section, the FMECA of each subsystem is shown in detail. The subsystems are the ACS, ADS, CDH, EPS, TT&C, and structures. By performing the FMECA for each subsystem, different failures modes from the SwampSat mission FMECA were identified. Table B-1 shows the ACS subsystem FMECA and Table B-2 shows the ADS subsystem FMECA. Tables B-3 and B-4 show the FMECA for the CDH and the EPS subsystems correspondingly. The TT&C subsystem FMECA is shown in Table B-5 and the FMECA for the structures is shown in Table B-6.

Table B-1. ACS subsystem FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
CMG failure	Insufficient power	Unable to generate enough torque to perform attitude maneuvers	1	4	4 (Low)	SwampSat goes in to Safe-Hold mode	The battery can be recharged from the solar cells
	CMG pyramid configuration breaks due to environment conditions	Unable to perform attitude maneuvers	5	5	25 (High)	No change in downlink telemetry from SwampSat	Environmental testing before launch
Flywheel failure	Bearing contamination	Unable to perform attitude maneuvers	5	5	25 (High)	No flywheel data from SwampSat downlink	Apply lubricant for the bearing.
	Motor failure	Unable to perform attitude maneuvers	5	5	25 (High)	No flywheel data from SwampSat downlink	Functionality testing before launch
	Slip ring failure	Unable to perform attitude maneuvers	5	5	25 (High)	No flywheel data from SwampSat downlink	Functionality testing before launch
	Cold welding	Unable to perform attitude maneuvers	5	5	25 (High)	No flywheel data from SwampSat downlink	Proper vacuum testing before launch
	Speed sensor failure	Unable to obtain flywheel speed	4	5	20 (High)	No flywheel speed data from SwampSat downlink	Functionality testing before launch
	Flywheel assembly breaks due to environment conditions	Unable to perform attitude maneuvers	5	5	25 (High)	No flywheel data from SwampSat downlink	Environmental testing before launch

Table B-1. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Gimbal failure	Bearing contamination	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Apply lubricant for the bearing.
	Motor failure	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Functionality testing before launch
	Bearing contamination	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Apply lubricant for the bearing.
	Cold welding	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Proper vacuum testing before launch
	Encoder failure	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Run software during testing to ensure algorithm is working
	Cable failure	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Functionality testing before launch
	Position sensor failure	Unable to obtain gimbal position	4	5	20 (High)	No gimbal position from SwampSat downlink	Functionality testing before launch
	Gimbal assembly breaks due to environmental conditions	Unable to perform attitude maneuvers	5	5	25 (High)	No gimbal data from SwampSat downlink	Environmental testing before launch
Motor driver board failure	Master motor driver board failure	Unable to perform CMG operations	5	5	25 (High)	No MDB data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table B-1. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Motor driver boar failure	Slave motor driver board failure	Unable to perform CMG operations	5	5	25 (High)	No MDB data from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
	Motor driver board temperature sensor failure	Unable to downlink temperature of motor driver board	1	2	2 (Low)	No MDB temperature data from SwampSat downlink	Functionality testing before launch
	Programming error or runtime error	Unable to perform attitude maneuvers	5	4	20 (High)	No telemetry from SwampSat downlink	Run software during testing to ensure algorithm is working
CMG control software and steering logic failure	Programming error	Unable to execute QUEST, EKF, CMG control, and singular avoidance algorithms	5	4	20 (High)	No attitude telemetry from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working
Magnet coils failure	Insufficient power	Unable to turn the power on of the magnet coils.	1	4	4 (Low)	IMU rates are high and the Flag = Failure	Continuous monitoring and wait until sufficient power
	Malfunction of the load switch	Unable to turn the power the magnet coils. Result in no generation of magnetic field	5	2	10 (Mod)	IMU rates are high and the Flag =Failure	Functionality testing before launch
	PCB panels failure due to environment conditions	Unable to use magnet coils, no power generation from solar cells	5	3	15 (High)	No communication from SwampSat	Environmental testing before launch

Table B-1. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Magnet coils failure	Insufficient magnetic field generation	Unable to detumble SwampSat due to weak magnetic field generation	5	2	10 (Mod)	IMU rates are high and the Flag = Failure repetitively	Functionality testing, simulation, and analysis before launch
CMG controller failure	EEPROM on CMG controller malfunction	SFC430 unable to communicate with MBD and read from Flash of CMG controller	5	4	20 (High)	No data from MDB	Functionality testing and run software during testing to ensure algorithm is working
	Components (flywheel motor control board, gimbal motor control board, SPI signal interface) failure due to environmental condition	CMG Controller unable to operate; Unable to perform attitude maneuvers	5	2	10 (Mod)	No attitude telemetry from SwampSat downlink	Environment testing before launch
	Software error	Unable to perform attitude maneuvers	5	4	20 (High)	No IMU rates from SwampSat downlink	Run software during testing to ensure algorithm is working
Communication to CMG controller failure	SPI signal error	SFC430 unable to read IMU rates from Flash on CMG controller	5	2	10 (Mod)	No IMU rates and Launch Flag =0 from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table B-2. ADS subsystem FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Sun sensor failure	Burns out due to radiation damage	Unable to obtain Sun Sensor measurements to figure out the sun vector	5	5	25 (High)	Unable to obtain Sun sensor data from SwampSat downlink	Environmental testing before launch
	Saturates due to filter failure	Unable to obtain Sun Sensor measurements to figure out the sun vector	5	5	25 (High)	Able to determine that the Sun sensor has saturated from the downlink data	Functionality testing before launch
	Sun sensor breaks due to environmental conditions	Unable to obtain Sun Sensor measurements to figure out the sun vector	5	5	25 (High)	Unable to obtain Sun sensor data from SwampSat downlink	Environmental testing before launch
Magnetometer (HCM2003) failure	Burns out due to power bus spike	Unable to obtain magnetometer measurements to figure out magnetic field vector	5	2	10 (Mod)	Unable to obtain magnetometer data from SwampSat downlink	Functionality testing before launch
	Magnetometer breaks due to environmental conditions	Unable to obtain magnetometer measurements to figure out magnetic field vector	5	2	10 (Mod)	Unable to obtain magnetometer data from SwampSat downlink	Environmental testing before launch
Software error in ADS algorithms	Programming error	Unable to validate ADS subsystem	5	4	20 (High)	Unable to obtain ADS telemetry from SwampSat downlink	Run software during testing to ensure algorithm is working

Table B-2. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
IMU ADIS16405 failure	Insufficient power	Unable to take IMU measurements	1	4	4 (Low)	Unable to receive IMU rates from SwampSat	Continuous monitoring and wait until sufficient power
	IMU temperature sensor failure	Unable to downlink temperature data of IMU	1	2	2 (Low)	Unable to obtain IMU temperature data from SwampSat	Functionality testing before launch
	SPI signal error	CMG controller unable to read IMU data	5	2	10 (Mod)	Unable to receive IMU rates from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
	IMU breaks due to environmental conditions	Unable to take IMU measurements	5	2	10 (Mod)	Unable to receive IMU rates from SwampSat	Environmental testing before launch
A/D converters failure	Insufficient power	Unable to perform analog to digital conversion	1	4	4 (Low)	Able to determine failure from the downlink data	Continuous monitoring and wait until sufficient power
	A/D converter breaks due to environmental conditions	Unable to perform analog to digital conversion	5	2	10 (Mod)	Able to determine failure from the downlink data	Environmental testing before launch
	Programming error	Unable to perform analog to digital conversion	5	4	20 (High)	Able to determine failure from the downlink data	Run software during testing to ensure algorithm is working

Table B-3. CDH subsystem FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Flight computer failure	Insufficient power	Unable to operate SwampSat	1	3	3 (Low)	No communications with SwampSat	Continuous monitoring and wait until sufficient power
	Components failure (i.e., MSP 430 microcontroller, HMC2003 magnetometer, burn wire load switch, magnet coil load switch, backup magnet coil circuit, magnetometer set/reset circuit, I2C peripheral bus, SwampSat electrical bus RBF switch, deployment switch interface, USB port, JTAG connection, DC power jack, ACS-Comms cable interface)	Unable to operate SwampSat	5	3	15 (High)	No communications with SwampSat	Functionality testing and run software during testing to ensure algorithm is working
	SFC-430 breaks due to environmental conditions	Unable to operate SwampSat	5	4	20 (High)	No communications with SwampSat	Environmental testing before launch
	MSP 430 temperature sensor failure	Unable to downlink temperature data of MSP 430 from SwampSat	1	2	2 (Low)	Unable to obtain temperature data of MSP 430 from SwampSat downlink	Functionality testing before launch

Table B-3. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
SFC430 failure	Software error in SFC-430 algorithm	Unable to collect health data Unable to command Stensat Unable to convert analog data to digital. Unable to power the magnet coils. Unable to communicate with TI DSP.	5	4	20 (High)	No communication with SwampSat	Run software during testing to ensure algorithm is working
RTC failure	I2C signal error	Unable to access real time data	5	2	10 (Mod)	Unable to downlink SwampSat real time data	Ground testing before launch
	RTC breaks due to environment conditions	Unable to access real time data	5	1	5 (Low)	Unable to downlink SwampSat real time data	Environmental testing before launch
EEPROM failure	I2C signal error	Unable to store any data	5	2	10 (Mod)	Unable to downlink any data from SwampSat	Ground testing before launch
	Flash breaks due to environment conditions	Unable to store any data	5	1	5 (Low)	Unable to downlink any data from SwampSat	Environmental testing before launch
Boot count failure	Insufficient power	MSP 430 will remain off until it gets power	1	4	4 (Low)	No data received from SwampSat	Continuous monitoring and wait until sufficient power
	Watchdog reset error	SFC430 unable to reboot	2	4	8 (Low)	Same data received from SwampSat.	Run software during testing to ensure algorithm is working

Table B-3. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Boot count failure	Software error	SFC430 unable to reboot and cannot get out of infinite loop	1	4	4 (Low)	Same data received from SwampSat SwampSat does not respond to commands	Run software during testing to ensure algorithm is working
Query beacon failure	I2C signal error	Unable to read EPS telemetry, RTC, transceiver telemetry, boot count, boot time, and Flash	5	2	10 (Mod)	No EPS data, Comms data, real-time data, boot count and boot time data	Functionality testing and run software during testing to ensure algorithm is working
	SPI signal error	Unable to read IMU rates, IMU temperature, MDB temperature	5	2	10 (Mod)	No CMG data in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
	ADC signal error	Unable to read SFC430 temperature sensor	5	2	10 (Mod)	No temperature sensor data in downlink from SwampSat	Functionality testing and run software during testing to ensure algorithm is working
	Software error	Unable to query beacon	5	4	20 (High)	Unable to downlink real time data from SwampSat	Run software during testing to ensure algorithm is working
Software error in CDH algorithm	Programming error	Unable to operate SwampSat	5	4	20 (High)	No communication with SwampSat	Run software during testing to ensure algorithm is working

Table B-4. EPS subsystem FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Clyde Space EPS board failure	Lithium ion battery failure	Once the battery is discharged, it will not able to recharge	5	2	10 (Mod)	No communication with SwampSat	Functionality testing before launch
	Components on the EPS board breaks due to environment conditions	Unable to generate any power for SwampSat	5	1	5 (Low)	No communication with SwampSat	Environmental testing before launch
	Battery temperature sensor failure	Unable to downlink battery temperature from SwampSat	1	2	2 (Low)	Unable to obtain battery temperature data from SwampSat	Functionality testing before launch
Solar cells failure	Solar cells malfunction	Unable to recharge the batteries using the solar cells	5	2	10 (Mod)	No power available for SwampSat. No communication with SwampSat	Functionality testing before launch
	Solar cells breaks due to environment conditions	Unable to recharge the batteries using the solar cells	5	3	15 (High)	No power available for SwampSat. No communication with SwampSat	Environmental testing before launch
	Epoxy bonding not secured properly	No connection between the solar cells and the gold pad	5	3	15 (High)	No power available for SwampSat. No communication with SwampSat	Functionality testing before launch. Perform multiple tests to ensure the connection is secure
	Silver wire for electrical connection not secured properly	No connection between the solar cells and the gold pad	5	3	15 (High)	No power available for SwampSat. No communication with SwampSat	Functionality testing before launch. Perform multiple tests to ensure the connection is secure

Table B-4. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Solar Cells Failure	PCB breaks due to environment conditions	Unable to generate any power for SwampSat	5	2	10 (Mod)	No power available for SwampSat. No communication with SwampSat	Environment testing before launch
PCB Solar Panel Failure	PCB Panels breaks due to environment conditions	Solar cells on the PCB will also break and no power generation	5	3	15 (High)	No communication from SwampSat	Environment testing before launch
	Temperature sensors on PCB fail	Unable to downlink temperature data	1	3	3 (Low)	Unable to obtain temperature data from SwampSat	Functionality testing before launch
Communication with SFC430	I2C signal error	Unable to provide power information to SFC430	5	2	10 (Mod)	No power information from SwampSat downlink	Functionality testing and run software during testing to ensure algorithm is working

Table B-5. TT&C subsystem FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Antenna failure	Short circuit due to contact with SwampSat structure	Impairs communication with SwampSat	5	2	10 (Mod)	Unable to downlink and uplink data to SwampSat	Ground testing before launch. Using Delrin plate and the rails are hard anodized to prevent any short circuit.
	Antenna prematurely deploy due to vibration loads during launch	Impairs communication with SwampSat Interfere with deployment from P-POD	5	3	15 (High)	Unable to downlink and uplink data to SwampSat	Environment testing before launch. Perform multiple tests to ensure proper antenna deployment
	Failure in the co-axial cable due to shock and vibrations	Antenna will function but no communication within SwampSat	5	2	10 (Mod)	Antenna will function but no data from SwampSat	Functionality testing before launch
Antenna system failure	Receive antenna module failure	Unable to receive commands from ground station	5	3	15 (High)	SwampSat does not respond to ground commands	Functionality testing before launch
	Transmit antenna module failure	Unable to downlink to the ground station	5	3	15 (High)	SwampSat unable to transmit and the ground will not receive data	Functionality testing before launch
Transceiver Board Failure	Components (Transceiver, I2C signal interface, electrical interface) are useless due to environment conditions	Unable to receive and transmit data	5	2	10 (Mod)	Unable to downlink and uplink data to SwampSat	Environmental testing before launch

Table B-5. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Receive antenna module failure	Delrin plate failure	Unable to hold the antenna mechanism	5	2	10 (Mod)	SwampSat unable to receive commands from ground station	Functionality testing before launch
	Nitinol dipole antenna element failure	Unable to use the antenna element as antenna to receive commands	5	3	15 (High)	SwampSat unable to receive commands from ground station	Functionality testing before launch
	Interface failure	No connection between interfaces	5	3	15 (High)	No communicati on with SwampSat	Functionality testing before launch
	Receive antenna module failure due to environment conditions	SwampSat unable to receive commands	5	2	10 (Mod)	SwampSat does not respond to ground commands	Environmental testing before launch
Transmit antenna module failure	Delrin plate failure	Unable to hold the antenna mechanism	5	2	10 (Mod)	SwampSat unable to downlink to ground station	Functionality testing before launch
	Nitinol dipole antenna element failure	Unable to use the antenna element as antenna to transmit	5	3	15 (High)	SwampSat unable to downlink to ground station	Functionality testing before launch
	Interface failure	No connection between interfaces	5	3	15 (High)	No communicati on with SwampSat	Functionality testing before launch
	Transmit antenna module failure due to environment conditions	No downlink from SwampSat	5	2	10 (Mod)	SwampSat unable to downlink to ground station	Environmental testing before launch

Table B-5. Continued

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Software error in telemetry algorithm	Programming error	Unable to access real time data for any operations. Unable to store operation data for each mode	5	4	20 (High)	Unable to downlink and uplink data to SwampSat	Run software during testing to ensure algorithm is working
Ground station failure	Malfunction of the equipment (Antenna element, antenna rotor, rotor computer controller, transceiver, and Terminal Node Controller (TNC))	Unable to uplink commands to SwampSat and downlink from SwampSat	5	1	5 (Mod)	Visually recognize failure in the equipment	Functionality testing and check equipment regularly

Table B-6. Structures FMECA

Hypothetical failure mode	Hypothetical failure cause	Hypothetical potential effects	Severity (1-5)	Likelihood (1-5)	Criticality	Detection method	Preventative action
Side 1, Side 3, or bottom plate failure	The structure breaks due to environment conditions	The structure will fall apart	5	1	5 (Mod)	No communication from SwampSat	Environment testing before launch
Side 2, Side 4 delrin X-plates failure	The structure breaks due to environment conditions	The structure will fall apart	5	1	5 (Mod)	No communication from SwampSat	Environment testing before launch
Interface failure	The fasteners between the bottom plate and the CMG may become loose due to vibrations	CMG will move and cannot perform CMG maneuvers. There will also be high vibration	5	3	15 (High)	Unable to perform CMG maneuver, high rates from the IMU	Vibration testing before launch and securing the fasteners with loctite
	The fasteners between the delrin plates /PCB panels may become loose due to vibrations	If some become loose, the structure will still remain rigid and no potential harm to the mission	3	3	9 (Mod)	No certain way to detect that the fasteners have become loose or not	Vibration testing before launch and securing the fasteners with loctite
	The epoxy might fail due to environment conditions	The cables wil become loose but no potential harm to the mission	1	3	3 (Low)	No certain way to detect this has occurred	Environment testing before launch of the epoxy
	The wires soldered to the PCB panel not secured properly	No electrical connection	5	3	15 (High)	No communication from SwampSat	Layer of epoxy will be placed on top of the solder
	Cabling failure, no secure connection between interfaces	No electrical connection	5	3	15 (High)	No communication from SwampSat	Functionality testing before launch
RBF pin failure	Mechanism failure	Unable to power up the EPS launched	3	3	9 (Mod)	Able to detect failure before launch	Build RBF switch according to CDS. Functionality testing

APPENDIX C
DOWNLINK TELEMETRY DATA

In this section, the downlink telemetry data for the entire SwampSat mission is shown. Table C-1 shows the SwampSat Beacon; Safe-hold mode downlink telemetry data. Table C-2 shows the detumble mode downlink telemetry data. Table C-3 shows the ADS mode downlink telemetry data. Finally Table C-4 shows the CMG Ops Mode downlink telemetry data. Using the downlink telemetry, the ground station will be able to identify any failures during each operating mode. Detailed explanation for the SwampSat downlink telemetry data, see the SwampSat TT&C design document [5, 37].

Table C-1. SwampSat beacon; Safe-Hold mode downlink telemetry data

Quantity	Hardware	Interface	Bits	Hex Characters
time stamp				
year	RTC	I2C	12	3
month	RTC	I2C	4	1
date	RTC	I2C	8	2
hour	RTC	I2C	8	2
minute	RTC	I2C	8	2
seconds	RTC	I2C	8	2
MMDB temperature 1	TI-DSP	SPI	12	3
MMDB temperature 2	TI-DSP	SPI	12	3
SMDB temperature 1	TI-DSP	SPI	12	3
SMDB temperature 2	TI-DSP	SPI	12	3
IMU X	IMU	SPI	14	4
IMU Y	IMU	SPI	14	4
IMU Z	IMU	SPI	14	4
IMU temperature	IMU	SPI	12	3
battery voltage	EPS	I2C	10	3
battery current	EPS	I2C	10	3
battery bus current	EPS	I2C	10	3
battery current direction	EPS	I2C	10	3
battery temperature	EPS	I2C	10	3
5V bus current	EPS	I2C	10	3
3.3V bus current	EPS	I2C	10	3
transmitter current	TCVR	I2C	10	3
receiver current	TCVR	I2C	10	3
boot count	EEPROM	I2C	12	3
boot time				
year	RTC	I2C	12	3
month	RTC	I2C	4	1
date	RTC	I2C	8	2
hour	RTC	I2C	8	2
minute	RTC	I2C	8	2
seconds	RTC	I2C	8	2
msp430 temperature	SFC430	A/D	12	3

Table C-2. Detumble mode downlink telemetry data

Quantity	Hardware	Interface	Bits	Hex Characters
time stamp				
year	RTC	I2C	12	3
month	RTC	I2C	4	1
date	RTC	I2C	8	2
hour	RTC	I2C	8	2
minute	RTC	I2C	8	2
seconds	RTC	I2C	8	2
IMU X	IMU	SPI	14	4
IMU Y	IMU	SPI	14	4
IMU Z	IMU	SPI	14	4
IMU temperature	IMU	SPI	12	3
solar cell voltage 1	EPS	I2C	10	3
solar cell voltage 2	EPS	I2C	10	3
solar cell voltage 3	EPS	I2C	10	3
solar cell voltage 4	EPS	I2C	10	3
solar cell voltage 5	EPS	I2C	10	3
solar cell current 1	EPS	I2C	10	3
solar cell current 2	EPS	I2C	10	3
solar cell current 3	EPS	I2C	10	3
solar cell current 4	EPS	I2C	10	3
solar cell current 5	EPS	I2C	10	3
side temperature 1	EPS	I2C	10	3
side temperature 2	EPS	I2C	10	3
side temperature 3	EPS	I2C	10	3
side temperature 4	EPS	I2C	10	3
side temperature 5	EPS	I2C	10	3
battery voltage	EPS	I2C	10	3
battery current	EPS	I2C	10	3
battery bus current	EPS	I2C	10	3
battery current direction	EPS	I2C	10	3
battery temperature	EPS	I2C	10	3

Table C-3. ADS mode downlink telemetry data

Quantity	Hardware	Interface	Bits	Hex Characters
time stamp				
year	RTC	I2C	12	3
month	RTC	I2C	4	1
date	RTC	I2C	8	2
hour	RTC	I2C	8	2
minute	RTC	I2C	8	2
seconds	RTC	I2C	8	2
IMU X	IMU	SPI	14	4
IMU Y	IMU	SPI	14	4
IMU Z	IMU	SPI	14	4
IMU temperature	IMU	SPI	12	3
magnetometer X	SFC430	I2C	12	3
magnetometer Y	SFC430	I2C	12	3
magnetometer Z	SFC430	I2C	12	3
sun sensor 1	SFC430	ADC	12	3
sun sensor 2	SFC430	ADC	12	3
sun sensor 3	SFC430	ADC	12	3
sun sensor 4	SFC430	ADC	12	3
sun sensor 5	SFC430	ADC	12	3
sun sensor 6	SFC430	ADC	12	3
quaternion q1	TI-DSP	SPI	64	16
quaternion q2	TI-DSP	SPI	64	16
quaternion q3	TI-DSP	SPI	64	16
quaternion q4	TI-DSP	SPI	64	16

Table C-4. CMG Ops mode downlink telemetry data

Quantity	Hardware	Interface	Bits	Hex Characters
time stamp				
year	RTC	I2C	12	3
month	RTC	I2C	4	1
date	RTC	I2C	8	2
hour	RTC	I2C	8	2
minute	RTC	I2C	8	2
seconds	RTC	I2C	8	2
IMU X	IMU	SPI	14	4
IMU Y	IMU	SPI	14	4
IMU Z	IMU	SPI	14	4
IMU temperature	IMU	SPI	12	3
MMDB temperature 1	TI-DSP	SPI	12	3
MMDB temperature 2	TI-DSP	SPI	12	3
SMDB temperature 1	TI-DSP	SPI	12	3
SMDB temperature 2	TI-DSP	SPI	12	3
flywheel speed 1	TI-DSP	SPI	12	3
flywheel speed 2	TI-DSP	SPI	12	3
flywheel speed 3	TI-DSP	SPI	12	3
flywheel speed 4	TI-DSP	SPI	12	3
gimbal rate 1	TI-DSP	SPI	12	3
gimbal rate 2	TI-DSP	SPI	12	3
gimbal rate 3	TI-DSP	SPI	12	3
gimbal rate 4	TI-DSP	SPI	12	3
gimbal angle 1	TI-DSP	SPI	12	3
gimbal angle 2	TI-DSP	SPI	12	3
gimbal angle 3	TI-DSP	SPI	12	3
gimbal angle 4	TI-DSP	SPI	12	3
magnetometer X	SFC430	I2C	12	3
magnetometer Y	SFC430	I2C	12	3
magnetometer Z	SFC430	I2C	12	3
sun sensor 1	SFC430	ADC	12	3
sun sensor 2	SFC430	ADC	12	3
sun sensor 3	SFC430	ADC	12	3
sun sensor 4	SFC430	ADC	12	3
sun sensor 5	SFC430	ADC	12	3
sun sensor 6	SFC430	ADC	12	3
quaternion q1	TI-DSP	SPI	64	16
quaternion q2	TI-DSP	SPI	64	16
quaternion q3	TI-DSP	SPI	64	16
quaternion q4	TI-DSP	SPI	64	16

REFERENCES

[1] Toorian, A., Blundell, E., Suari, J., and Twiggs, R., “CubeSats as Responsive Satellites,” Paper no. AIAA-RS3 2005-3001, AIAA 3rd Responsive Space Conference, Los Angeles, CA, April 2005.

[2] Puig-Suari, J., Turner, C., and Ahlgren, W., “Development of the Standard CubeSat Deployer and a CubeSat Class PicoSatellite,” Aerospace Conference, 2001, IEEE Proceedings., Vol. 1, 2001, pp. 347-353

[3] Nugent, R., Coelho, R., Munakata, R., Chin, A., and Puig-Suari, J., “The CubeSat: The Picosatellite Standard for Research and Education,” Paper no. AIAA-2008-7734, AIAA SPACE 2008 Conference and Exposition, San Diego, California, Sep. 2008.

[4] Munkata, R., “CubeSat Design Specification Rev. 12,” August, 2009.

[5] Leve, F., Allgeier, S., Nagabhushan, V., Asundi, S., Buckley, D., Waldrum, A., and Hiramatsu, T., “ASTREC-I Detailed Design Report, FUNSAT IV Design Competition,” 2007–2008.

[6] Nagabhushan, V., *Development of Control Moment Gyroscopes for Attitude Control of Small Satellites*, Master’s thesis, University of Florida, 2009.

[7] Asundi, S., *CubeSat System Design Based on Methodologies Adopted for Developing Wireless Robotic Platform*, Ph.D. thesis, University of Florida, 2011.

[8] Santoni, F., “Risk Management for Micro-Satellite Design,” Acta Astronautica, Vol. 54, 2003, pp. 221-228.

[9] “SMC Systems Engineering Primer & Handbook,” 3rd ed., Space & Missile Systems Center, U.S. Air Force, April 2005.

[10] Hecht, H., “Analytical Approaches to Failure Prevention,” *Systems Reliability and Failure Prevention*, Artech House, Massachusetts, 2004, pp. 37-61.

[11] Birolini, A., *Reliability Engineering: Theory and Practice*, 5th ed., Springer, New York, 2007.

[12] “NASA Systems Engineering Handbook,” NASA/SP-2007-6105, Dec. 2007.

[13] Dussault, H. B., “The Evolution and Practical Applications of Failure Modes, and Effects Analyses,” RADC-TR-83-72, *Air Force Systems Command*, August 1983.

[14] “Technical Manual: Failure Modes, Effects and Criticality Analyses (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and

Reconnaissance (C4ISR) Facilities," Department of Army, TM 5-698-4, Sept. 2006.

[15] "Procedures for Performing a Failure Mode, Effects, and Criticality Analysis," Department of Defense MIL-STD-1629A, Nov. 1980.

[16] "Risk Assessment," *LOFAR Austin Meeting*, NASA, March 2002.

[17] "XFMEA," *ReliaSoft Corporation Worldwide Headquarters,* http://www.reliasoft.com/pubs/xfmea_brochure.pdf, [retrieved June 10 2011]

[18] Ericson, C. A., "Fault Tree Analysis," *Presentation*, The Boeing Company, Sept. 2000.

[19] Ericson, C.A., "Fault Tree Analysis – A History," *Proceedings of The 17th International System Safety Conference*, The Boeing Company, August 1999.

[20] Rausand, M., "System Analysis: Fault Tree Analysis," *Norwegian University of Science and Technology*, http://www.ntnu.no/ross/srt/slides/fta.pdf, [retrieved Sept. 23 2010]

[21] Rausand, M., and Hoyland, A., *System Reliability Theory: Models, Statistical Methods and Applications,* 2nd ed., Wiley, New Jersey, 2004.

[22] "BlockSim 7," *ReliaSoft Corporation Worldwide Headquarters,* http://www.reliasoft.com/pubs/blocksim_brochure.pdf, [retrieved June 10 2011]

[23] "Appendix J. Technology Readiness Levels (TRLs)," NPR 7120.8, NASA, Feb. 2008.

[24] Nagabhushan, V., "SwampSat Mission Requirements and Traceability," 2009.

[25] "A Brief Chronology of Amateur Satellites," *AMSAT*, http://www.amsat.org/amsat-new/satellites/history.php, [retrieved Sept. 3 2010]

[26] "Guide to Reusable Launch and Reentry Vehicle Software and Computing System Safety," *FAA Commercial Space Transportation*, July 2006.

[27] Munkata, R., "CubeSat Acceptance Checklist Rev. 12," August, 2009.

[28] Lan, W., "Poly Picosatellite Orbital Deployer Mk III ICD," http://cubesat.calpoly.edu/images/LaunchProviders/mk iii icd5.pdf, 2007. [retrieved Sept. 3 2010]

[29] Lee, S., Toorian, A., Clemens, N., Puig-Suari, J., and Twiggs, B., "Cal Poly Coordination of Multiple CubeSats on the DNEPR Launch Vehicle," 18th Annual

AIAA/USU Conference on Small Satellites, Utah, August 2004.

[30] "MSP430™16-bit Ultra-Low Power MCUs," *Texas Instruments Inc.,* http://focus.ti.com/mcu/docs/mcumspoverview.tsp?sectionId=95&tabId=140&familyId=342, [retrieved Dec 9 2010].

[31] "Electrical Power Systems," *Clyde Space*, http://www.clyde-space.com/products/electrical_power_systems, [retrieved June 8 2011]

[32] Buckley, D. A., *SwampSat Antenna System*, Master's thesis, University of Florida, 2009.

[33] "ADIS16405: High Precision Tri-Axis Inertial Sensor with Magnetometer," *Analog Devices Inc.*, http://www.analog.com/static/imported-files/data_sheets/ADIS16405.pdf, [retrieved Dec 9 2010].

[34] "C6000 High Performance DSP," *Texas Instruments Inc.,* http://focus.ti.com/paramsearch/docs/parametricsearch.tsp?family=dsp&sectionId=2&tabId=57&familyId=132, [retrieved Dec 9 2010].

[35] "3-Axis Magnetic Sensor Hybrid HMC2003," *Honeywell,* http://www51.honeywell.com/aero/common/documents/myaerospacecatalog-documents/Missiles-Munitions/HMC_2003.pdf, [retrieved Dec 9 2010].

[36] "AD7994: 4 Channel, 12-Bit ADC with I^{2}C Compatible Interface in 16-Lead TSSOP," *Analog Devices*, http://www.analog.com/static/imported-files/data_sheets/AD7993_7994ERRATA.pdf, [retrieved Dec 9 2010].

[37] Allgeier, S., Asundi, S., Mahin, M., and Lin, T. Y., "SwampSat Telemetry Format," August 2010

BIOGRAPHICAL SKETCH

Bungo Shiotani was born on the seventeenth day of June in the year nineteen eighty five in Osaka, Japan. At the age of 6, he moved to Hong Kong with his family. Originally, the family was to live in Hong Kong for a year, however, he and his family lived there for 7 years. In Hong Kong, he first learned British English, since Hong Kong was still a British colony. At the age of 13, he moved back to Japan and decided to enroll in an international school in Kobe. Bungo kept studying English at the international school while his older brother attended a local Japanese junior high school. Bungo graduated high school from the international school in 2003 and decided to continue his studies in the United States.

In August 2003, he attended Jacksonville University where he enrolled in a 5 year dual degree Bachelor of Science engineering program. The first 3 years were to be studied at Jacksonville University and the last 2 years to be completed at an affiliated institution. After completing 3 years at Jacksonville, Bungo decided to attend the University of Florida. In 2008, he graduated with Bachelor of Science in Aerospace Engineering from the University of Florida and Bachelor of Science in Engineering Physics from Jacksonville University. He searched for aerospace related jobs in the United States, however, being an international student from Japan, he was unsuccessful. In 2009, he decided to continue his academic career and was accepted to pursue his master’s degree in Aerospace Engineering. He joined Dr. Fitz-Coy and his Space Systems Group to help complete the SwampSat project. In August 2011, he graduated with Master of Science in Aerospace Engineering and will continue studying as a doctorate student with Dr. Fitz-Coy and SSG. One of his goals will be to successfully send SwampSat into space.