A Systematic Risk Management Approach Employed on the CloudSat Project[1][2]

Ralph R. Basilio, Kim S. Plourde, and Try Lam
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, California 91109-8099
818.354.3228, 818.354.0087, and 818.354-6901
Ralph.R.Basilio@jpl.nasa.gov, Kim.S.Plourde@jpl.nasa.gov, and Try.Lam@jpl.nasa.gov

Abstract— The CloudSat Project has developed a simplified approach for fault tree analysis and probabilistic risk assessment. A system-level fault tree has been constructed to identify credible fault scenarios and failure modes leading up to a potential failure to meet the nominal mission success criteria. Risk ratings and fault categories have been defined for each low-level event (failure mode) and a streamlined version of the probabilistic risk assessment has been completed. Although this technique or process will mature and evolve on a schedule that emphasizes added value throughout the development life cycle, it has already served to confirm that project personnel are concentrating risk reduction or elimination/retirement measures in the appropriate areas. A cursory evaluation with an existing fault tree analysis and probabilistic risk assessment software application has helped to validate this simplified approach. It is hoped that this will serve as a model for other NASA flight projects.

TABLE OF CONTENTS

1. INTRODUCTION

As the prime NASA (National Aeronautics and Space Administration) center for the unmanned, robotic exploration of space, the Jet Propulsion Laboratory has employed a number of traditional techniques to identify and mitigate risks that could have deleterious effects on overall mission success. Typically, extensive ground-based verification and validation testing is combined with reliability evaluation techniques such as worst-case analyses and failure modes, effects, and criticality analyses.

In an effort to improve overall mission success probability, NASA now requires each project to enhance and augment its standard set of risk identification methods and mitigation procedures to include preparing both a system-level fault tree analysis and probabilistic risk assessment. The fault tree analysis provides for a systematic trace of the failure modes leading up to an undesired top-level event (i.e. mission failure); the probabilistic risk assessment is a quantitative comparison of potential risks, so that trade studies can be conducted and mitigation options examined.

Purpose

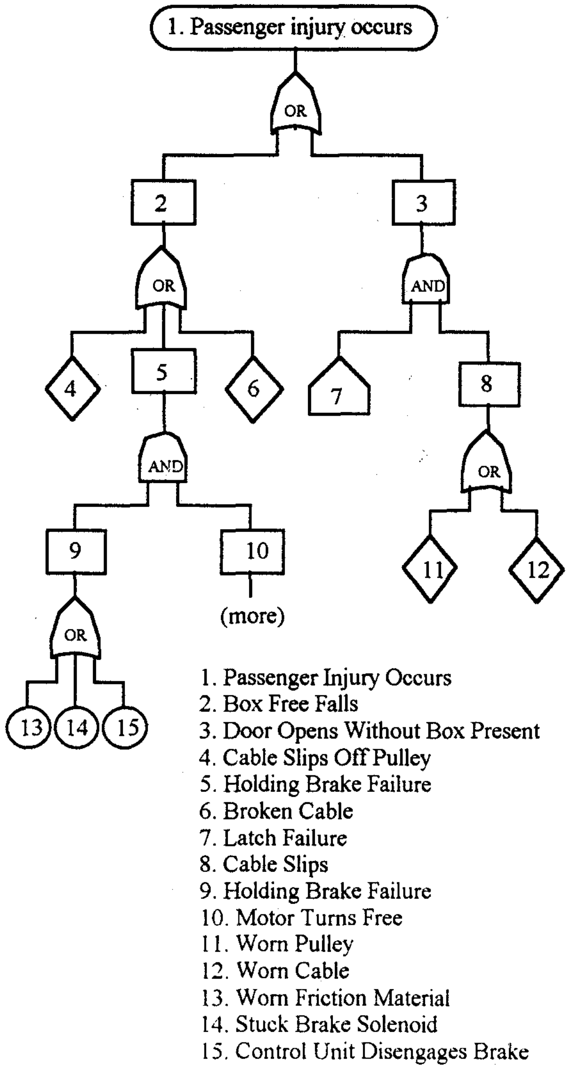
All space flight projects are challenged with developing and/or following a technique or approach that accommodates the enhanced risk mitigation initiative consistent with NASA's overall intent. To this end, the CloudSat Project has developed a simplified approach to both fault tree analysis and probabilistic risk assessment that enhances or augments the overall risk management program. This fault tree will evolve and mature to include links to worst-case analyses and failure modes, effects, and criticality analyses. Risks that can be reduced or retired through spacecraft system design changes (to include the addition of physical and/or functional redundancy) receive the most visibility at this stage of project development. Risks that remain after the design baseline is finalized are later addressed through development of contingency plans. In addition, any remaining, miscellaneous residual risks are also included on the project's significant risk list for close monitoring. This process will be completed on a schedule that emphasizes added value throughout the entire development life cycle, and takes into consideration both cost and schedule constraints. Before delving directly into CloudSat specifics, a general introduction of both fault tree analysis and probabilistic risk assessment are provided below.

[1] U. S. Government work not protected by U.S. copyright.

[2] Updated 18 October 2000

Fault Tree Definition

A fault tree is a graphical representation of the known faults or combinations of faults that will result in an undesired top-level event. Subordinate faults are linked through a series of logic "gates" that are similar to the logic gates that are frequently used in a typical engineering analysis. These gates permit or inhibit fault propagation to the next/higher level. There are a number of different logic gates, but two of the more frequently used are the OR gate and the AND gate. The OR gate is used to indicate that output to a fault event or transfer function occurs if one or more of the input events occurs. The AND gate is used to indicate that the output event occurs only if all input events occur. Fault tree generation and analysis is regarded as a top-down, systematic approach that entails the use of deductive reasoning. This approach involves the identification of a general top-level event and then developing a detailed set of possible causal events that eventually surface or manifest themselves as the top-level event. As with many other types of analysis this is a qualitative technique requiring one to understand the environment and the operations of the system, subsystem, and/or assembly being examined, so as to identify only credible scenarios. Identification and analysis of unrealistic events with only a remote possibility of occurrence may not only compromise the validity of results, but also overburden usually constrained cost and schedule resources.



1. Passenger Injury Occurs
2. Box Free Falls
3. Door Opens Without Box Present
4. Cable Slips Off Pulley
5. Holding Brake Failure
6. Broken Cable
7. Latch Failure
8. Cable Slips
9. Holding Brake Failure
10. Motor Turns Free
11. Worn Pulley
12. Worn Cable
13. Worn Friction Material
14. Stuck Brake Solenoid
15. Control Unit Disengages Brake

Figure 1 Example Fault Tree for Electromechanical Passenger Elevator [2]

Fault tree analysis enhances overall risk management by bringing to light likely, potential "show-stoppers". This technique is most effective when done early in the development life cycle (e.g. add in physical redundancy), but may still add significant value added when completed later (e.g. development of contingency plans). Finally, this top-down approach is used in conjunction with and complements any bottom-up analysis [e.g. FEMCA (Failure Modes, Effects, and Criticality Analysis].

Fault tree analysis is not a new technique. The NASA white paper on Guidelines for Program/Project Responsibilities for Safety and Mission Success [1] states that the Boeing Corporation first utilized this technique in 1964 to analyze potential faults associated with the Minuteman ICBM (Inter-Continental Ballistic Missile). More recently it has been used for the functional analysis of highly complex systems, evaluating system reliability, evaluating software interfaces, and identification of potential design defects and safety hazards.

An example fault tree taken from the Reliability Toolkit: Commercial Practices Edition [2] is shown in Figure 1. It shows the logical linking of events leading up to elevator passenger injury. Once can readily see that passenger injury can result from one of two events: the elevator car (box) free falls or the elevator door opens without the car being present. Let's examine the fault tree more closely.
In the case where the car free falls, there are three subordinate or causal faults: the cable slips off the pulley, the holding brake fails, and the cable breaks. A diamond symbol is used for the first and third faults to denote them as "undeveloped events", which means that even though the faults can be further decomposed they are regarded as the lowest level of examination for this purpose. In contrast, the "holding brake failure" has been decomposed to the point of identifying three basic events denoted by the circle symbol: worn friction material, stuck brake solenoid, and the control unit disengages the brake. One addition symbol that has not yet been described is the pentagon or "house". It contains a normal system operating input, but is regarded as an external event.

Finally, even though fault tree generation for a number of years since it's inception had been regarded as an art form it has been demonstrated time and time again that the most

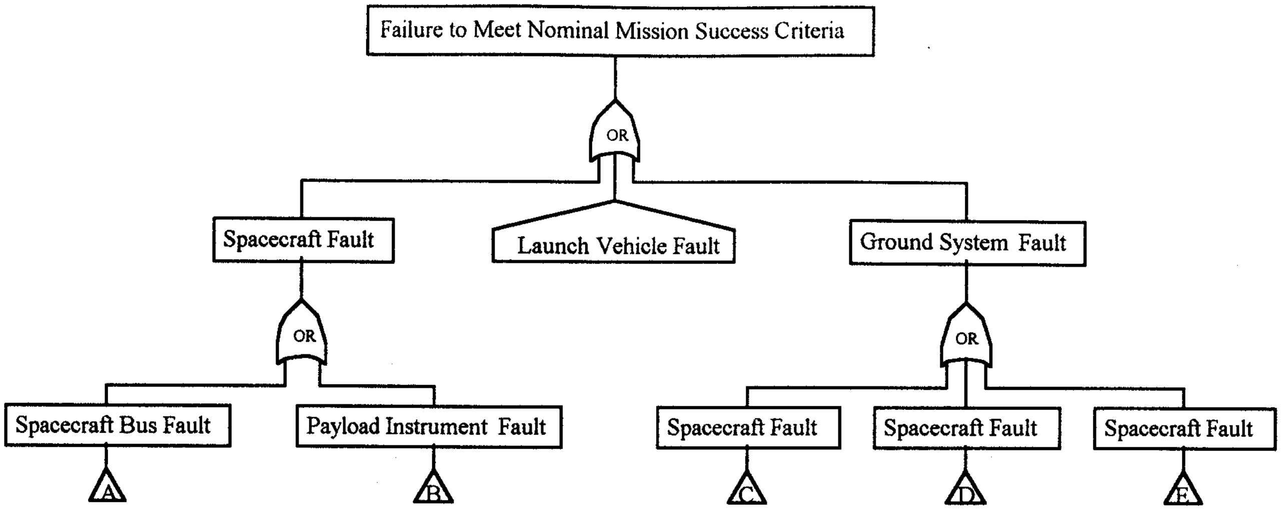


Figure 2 Top Level of CloudSat Fault Tree

accurate fault trees appear to conform to a set of guidelines. The Nuclear Regulatory Commission's Fault Tree Handbook [3] states five basic ground rules for fault tree construction which are given below.

Ground Rule I – Write the statements that are entered in the vent boxes as faults; state precisely what the fault is and when it occurs.

Ground Rule II – If the answer to the question, "Can this fault consist of a component failure?" is "Yes", classify the event as a "state-of-component fault". If the answer is "No", classify the event as a "state-of-system fault".

No Miracles Rule – If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.

Complete-the-Gate Rule – All inputs to a particular gate should be completely defined before further analysis of any one of them is undertaken.

No ,Gate-to-Gate Rule – Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates.

Probabilistic Risk Assessment Definition

Although fault tree analysis yields significant benefits it has limitations, not the least of which is the inability to predict likelihood of occurrence. Probabilistic risk assessment, which is a quantitative analysis technique, provides a complement to the more qualitative fault tree analysis. This technique involves the creation of a reliability model that utilizes the fault tree as an input. Expert judgement, operational experience, test data, and/or analysis are used to assign probabilities of occurrence and standard deviations. Probabilities are then assessed individually or combined according to the fault tree to identify "weak spots" and where to concentrate reliability options. Therefore, the key benefit in completing a probabilistic risk assessment is that it assists personnel with comparison or trade studies, so that resources can be allocated accordingly.

2. Mission Assurance Program

The objective of the CloudSat Project's mission assurance program is to identify, communicate, control, and mitigate potential risks to mission success. The challenge lies in achieving this objective in an efficient, yet effective manner that successfully accommodates the duai realities of finite program resources and high customer expectations.

The traditional approach to improving the efficiency of a project's risk mitigation activity focuses on streamlining planned verification and validation testing activities. This path is straightforward, conveniently lends itself to logic and the application of lessons learned, and usually produces tangible, quantifiable results. Often overlooked are the unrealized, potential gains in risk mitigation that may be obtained by improving upon analytical tools such as system-level fault tree analysis and probabilistic risk assessment.

In the following sections we describe the CloudSat Project's attempts to improve these tools and their methods of application

3. System-Level Fault Tree

In response to the NASA directive requiring the use of formal risk management processes and technologies, the

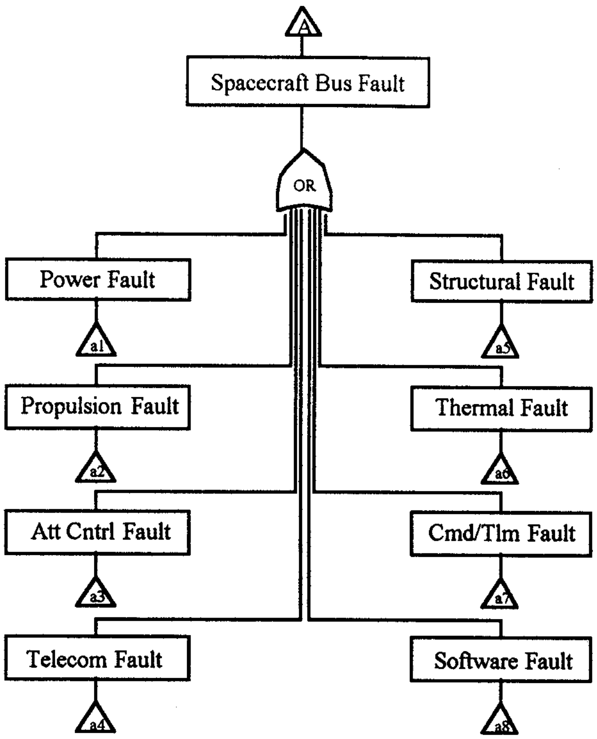


Figure 3 Spacecraft Bus (Subsystem) Faults

CloudSat Project will construct a system-level fault tree to identify credible fault scenarios and failure modes leading up to a postulated failure to meet the nominal mission objectives. Fault scenarios and failure modes to be considered include, but are not limited to interface faults (i.e. fault propagation), computer logic errors, environmental exposure, test, and test configuration errors.

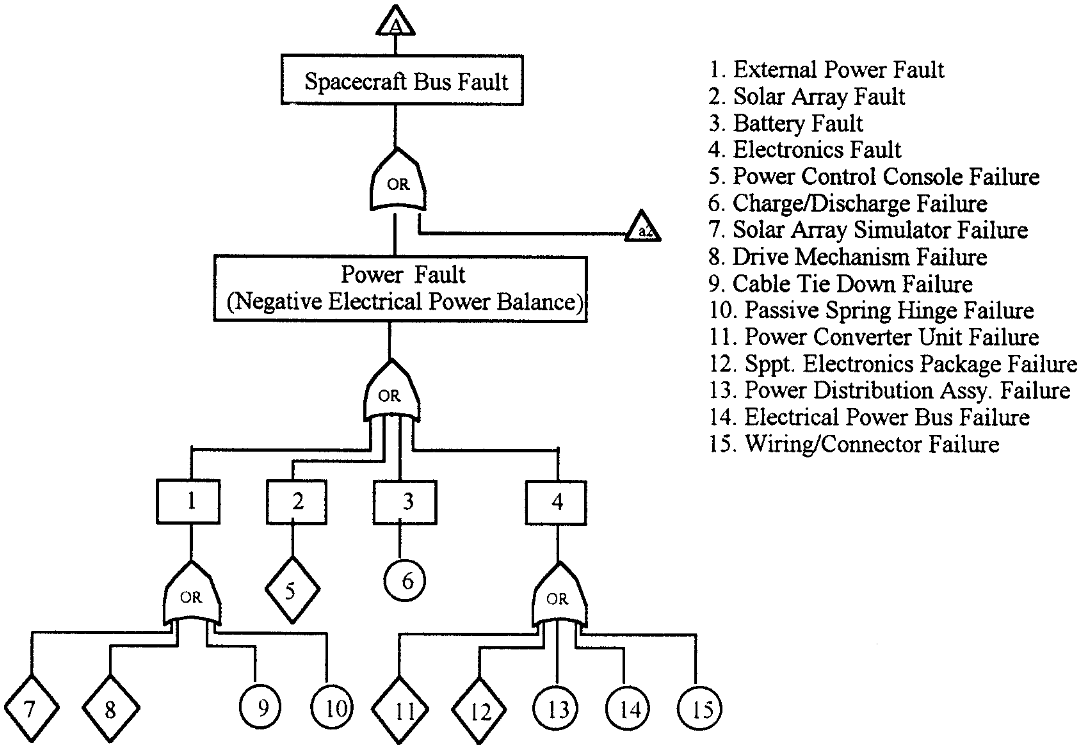
The high-level procedure for constructing the system-level fault tree is described below.

I. Definition – Define the top-level event, sub-ordinate fault scenarios, and failure modes

II. Linking – Link fault scenarios and failure modes with the appropriate logic gates.

Since construction of a system-level fault tree involves the definition of a considerable number of events and logic gates, the fault tree itself could not fit on a single, English standard 8-1/2in x 11in or metric A4 sheet of paper. In addition, the use of multiple sheets could lead one to become lost in a sea of paper. Finally, constructing the fault tree on larger "poster" size paper does not lend itself to portability and convenience. Therefore, a decision was made to construct the tree using a hyper-linked version of the Microsoft Powerpoint software application. This allowed each of the events and logic gates to remain legible and allowed one to move up and down the tree with relative ease using the hyperlinks.

The fault tree figures (nos. 2 through 8) are taken from the CloudSat fault tree constructed in its native Powerpoint



1. External Power Fault
2. Solar Array Fault
3. Battery Fault
4. Electronics Fault
5. Power Control Console Failure
6. Charge/Discharge Failure
7. Solar Array Simulator Failure
8. Drive Mechanism Failure
9. Cable Tie Down Failure
10. Passive Spring Hinge Failure
11. Power Converter Unit Failure
12. Sppt. Electronics Package Failure
13. Power Distribution Assy. Failure
14. Electrical Power Bus Failure
15. Wiring/Connector Failure

Figure 4 Negative Power Balance Fault Tree Branch

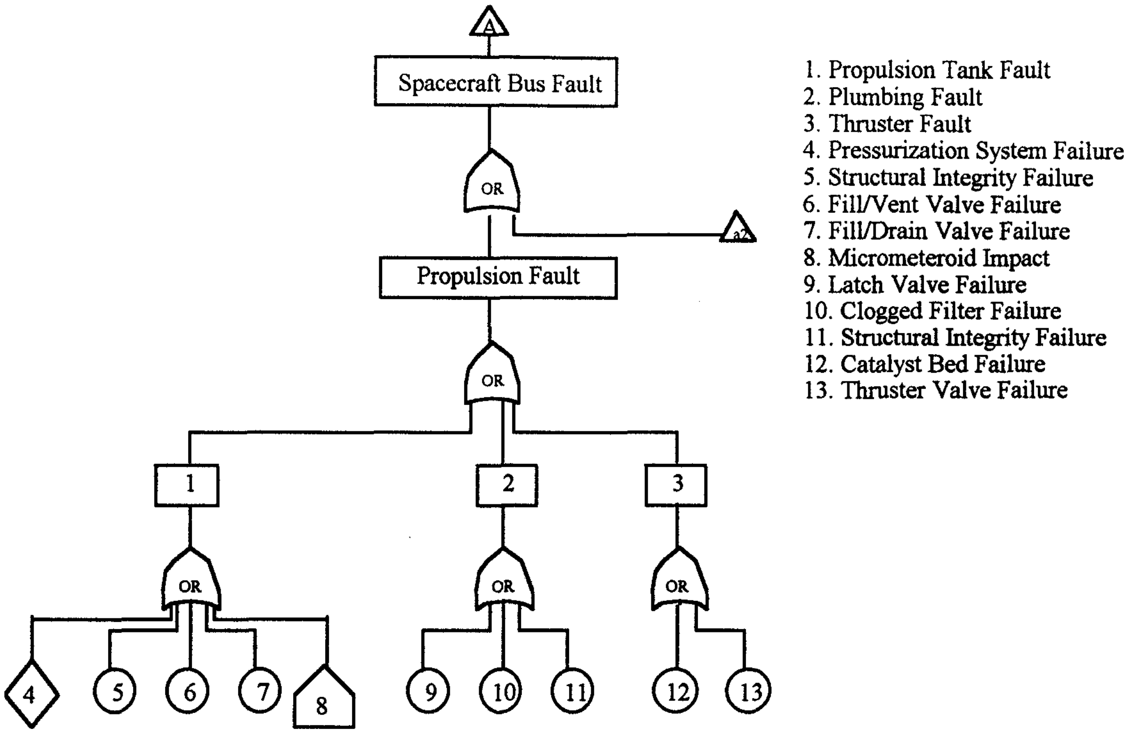

A
Spacecraft Bus Fault
OR
a2
Propulsion Fault
OR
1
2
3
OR
OR
OR
4
5
6
7
8
9
10
11
12
13
1. Propulsion Tank Fault
2. Plumbing Fault
3. Thruster Fault
4. Pressurization System Failure
5. Structural Integrity Failure
6. Fill/Vent Valve Failure
7. Fill/Drain Valve Failure
8. Micrometeroid Impact
9. Latch Valve Failure
10. Clogged Filter Failure
11. Structural Integrity Failure
12. Catalyst Bed Failure
13. Thruster Valve Failure

Figure 5 Propulsion Fault Tree Branch

format. Figure 2 shows the top-level of the fault tree indicating that a postulated failure to meet the nominal mission success criteria results from one of three potential faults: a spacecraft fault, a failure of the launch vehicle, and a ground system fault. Both the spacecraft and ground system faults are decomposed to indicate lower level faults. In the case of the spacecraft, the fault would originate from either the spacecraft bus or the payload instrument. If we

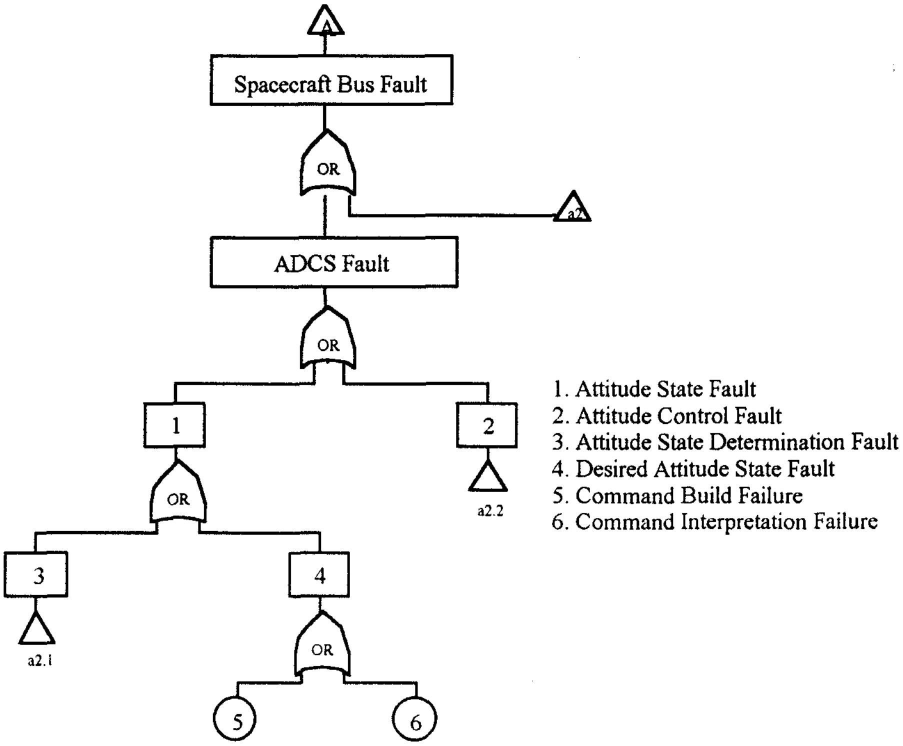
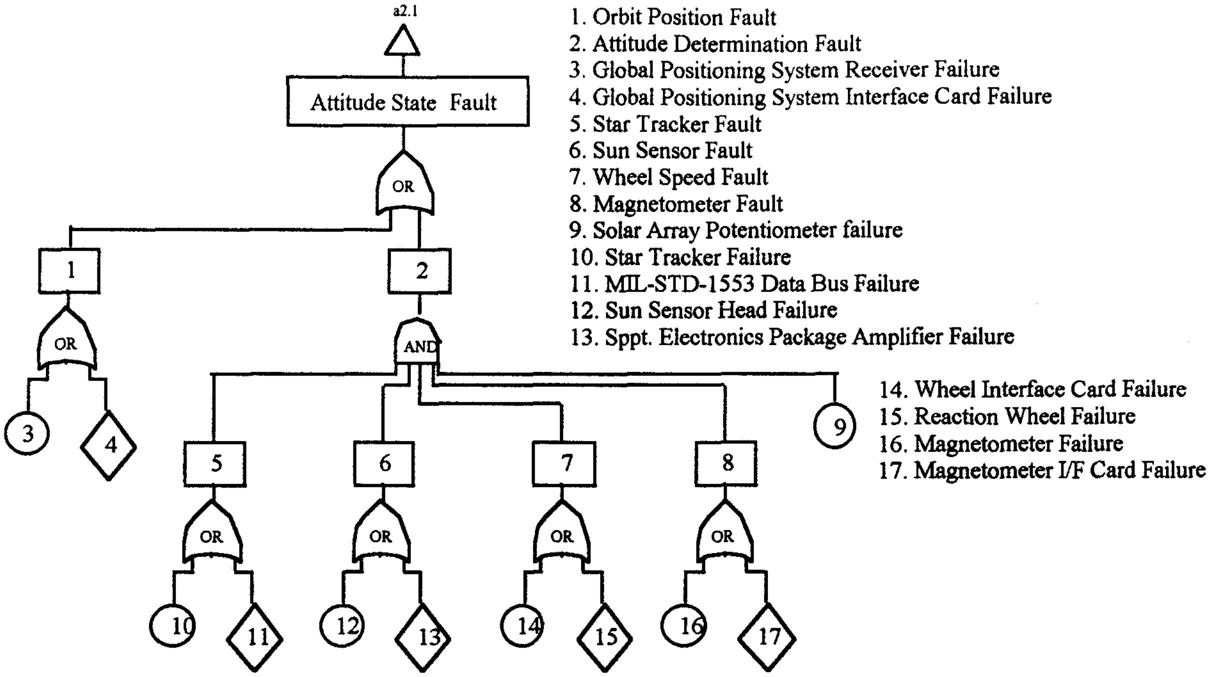

A
Spacecraft Bus Fault
OR
a2
ADCS Fault
OR
1
2
OR
a2.2
3
4
a2.1
OR
5
6
1. Attitude State Fault
2. Attitude Control Fault
3. Attitude State Determination Fault
4. Desired Attitude State Fault
5. Command Build Failure
6. Command Interpretation Failure

Figure 6 Attitude Determination and Control Main Fault Tree Branch

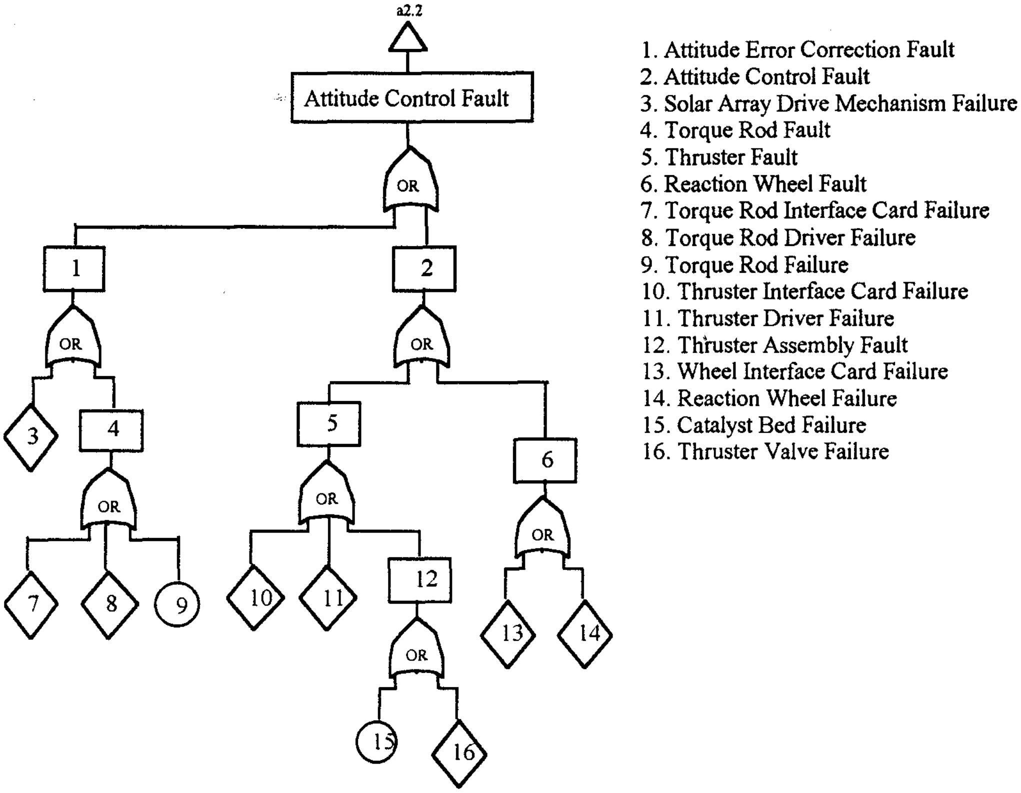


1. Orbit Position Fault
2. Attitude Determination Fault
3. Global Positioning System Receiver Failure
4. Global Positioning System Interface Card Failure
5. Star Tracker Fault
6. Sun Sensor Fault
7. Wheel Speed Fault
8. Magnetometer Fault
9. Solar Array Potentiometer failure
10. Star Tracker Failure
11. MIL-STD-1553 Data Bus Failure
12. Sun Sensor Head Failure
13. Sppt. Electronics Package Amplifier Failure
14. Wheel Interface Card Failure
15. Reaction Wheel Failure
16. Magnetometer Failure
17. Magnetometer I/F Card Failure

Figure 7 Attitude Determination and Control Fault Tree Branch "A"

take the spacecraft branch, this will lead us to the specific subsystems shown in Figure 3. From this point, we will investigate three subsystem faults in more detail: a power subsystem fault (negative power balance), a propulsion subsystem fault, and an attitude determination and control subsystem fault to assist in providing a better understanding of the subordinate fault scenarios and low-level failure modes.

Figure 4 shows the negative electrical power balance fault



1. Attitude Error Correction Fault
2. Attitude Control Fault
3. Solar Array Drive Mechanism Failure
4. Torque Rod Fault
5. Thruster Fault
6. Reaction Wheel Fault
7. Torque Rod Interface Card Failure
8. Torque Rod Driver Failure
9. Torque Rod Failure
10. Thruster Interface Card Failure
11. Thruster Driver Failure
12. Thruster Assembly Fault
13. Wheel Interface Card Failure
14. Reaction Wheel Failure
15. Catalyst Bed Failure
16. Thruster Valve Failure

Figure 8 Attitude Determination and Control Fault Tree Branch "B"

Electrical Power Fault (Negative Power Balance)

	Fault	Lower level fault or failure	Rating	Risk reduction or elimination measure(s)	Cat.
1	Ext Power Fault	Power Control Console failure	4	Heritage; checkout/certification prior to use	I
2	SA Fault	SA simulator failure	4	Heritage; checkout/certification prior to use	I
3		Release failure of cable tie down(s)	3	Heritage (IndoStar-1); ground test	IV
4		Failure of passive spring hinge(s)	3	Heritage (IndoStar-1); ground test	IV
5		Failure of drive mechanism(s)	3	Heritage; ground test	IV
6	Battery Fault	Charge/discharge failure	4	Heritage; ground test	IV
7	Electronics Fault	PCU failure	4	Internally redundant; heritage; ground test	II
8		PDA failure	4	Physically redundant; heritage; ground test	II
9		SEP failure	4	Functionally redundant; heritage; ground test	II
10		Bus failure	4	Physically redundant; heritage; ground test	II
11		Wiring/connector failure	6	Partially redundant; heritage; ground test	II

Table Ia Negative Power Balance Risk Ratings and Fault Catagories

tree branch. One can see that in addition to the solar array, battery, and electronics fault scenarios, a test configuration fault case involving the application of external power is also included for completeness. The solar array fault scenario contains primarily active mechanical failure modes, while the three other intermediate fault scenarios contain primarily active electrical failure modes. Events denoted by the circle again are those that are basic, low-level failure modes, while the events denoted by a diamond are those that can be decomposed further, but are not done at this stage of the project's development life cycle. It will be shown later with the final fault tree generation, that events denoted with a diamond will be linked to bottom-up analyses such a FMECA (Failure Mode, Effects, and Criticality Analysis).

Figure 5 shows the propulsion fault tree branch. One can see that active mechanical failure modes are contrasted with passive failure modes. It will be seen later in the probabilistic risk assessment section that there is vast difference in risk ratings between these two types of failures modes.

Finally, figures 6 through 8, show the attitude determination and control fault tree branch. Given the number of attitude determination and control subsystem assemblies and components, there are a considerable number of active electrical failure modes.

4. Probabilistic Risk Assessment

In response to the NASA directive requiring the use of formal risk management processes and technologies, the CloudSat Project will complete a relativistic probabilistic risk assessment to assist with the identification of residual risks and the application of 'appropriate' risk reduction or elimination/retirement actions. The probabilistic risk assessment will be conducted at the subsystem level.

The high-level procedure for completing the probabilistic risk assessment is described below.

For Each Failure Mode...

III. Risk Rating – Assign risk rating for each failure mode (lowest level fault). These risk ratings are equivalent to the

	Minimal Cut Set	Probability	Importance
A	3	1E-3	32.2%
B	4	1E-3	32.2%
C	5	1E-3	32.2%
D	6	1E-4	3.2%

Table Ib Negative Power Balance Minimal Cut Sets

Propulsion System Fault

	Fault	Lower level fault or failure	Rating	Risk reduction or elimination measure(s)	Cat.
1	Prop Tank Fault	Pressurization system failure	3	Heritage; certification prior to use	I
2		Structural integrity failure	6	Heritage; ground proof pressure and leak test	IV
3		Fill/vent valve failure	3	Heritage; ground leak test	IV
4		Fill/drain valve failure	3	Heritage; ground leak test	IV
5		Micro-meteoroid impact	6	None specified	IV
6	Plumbing Fault	Latch valve failure	3	One for each of two branches; ground test	II
7		Clogged filter	5	Check fuel contaminant level prior to loading	III
8		Structural integrity failure	6	Heritage; ground proof pressure and leak test	IV
9	Thruster Fault	Catalyst bed failure	5	Cat bed (and heater) for each of four thrusters	II
10		Thruster valve failure	3	Two on each of two branches; ground test	II

Table IIa Propulsion Fault Risk Ratings and Fault Catagories

rough order of magnitude failure probability and are described in more detail below.

"0": There is a 1E0 or one-in-one probability of occurrence for this completely deterministic event.

"1": There is a 1E-1 or one-in-ten probability of occurrence for this event.

"2": There is a 1E-2 or one-in-one-hundred probability of occurrence for this event.

"3": There is a 1E-3 or one-in-one-thousand probability of occurrence for this event. This is the threshold for 'active' mechanical components (e.g. actuators and springs).

"4": There is a 1E-4 or one-in-ten-thousand probability of occurrence for this event. This is the threshold for 'active' electrical components (e.g. relays and transistors).

"5": There is a 1E-5 or one-in-one-hundred-thousand probability of occurrence for this event.

"6": There is a 1E-6 or one-in-one-million probability of occurrence for this event. This is the threshold for 'passive' mechanical components (e.g. structural members).

IV. Actions Taken – State any risk reduction or elimination measure(s) already taken, if any.

V. Fault Categorization – Determine the appropriate fault category. It will be evident later that this is a key step in streamlining the overall process. Definitions for each of the four fault categories are derived from the Nuclear Regulatory Commission's Fault Tree Handbook [1] and are provided below.

"Level I": A negligible fault producing no impact to system performance or capability/capacity.

"Level II": A fault reducing overall system capacity, but does not impact on-line performance. An example of this is a failure of a physically redundant unit.

"Level III": A fault reducing overall system capacity and degrading on-line performance. An example of this is dual versus single-star tracker operations. The latter scenario will result in

	Minimal Cut Set	Probability	Importance
A	2	1E-6	0.1%
B	3	1E-3	49.9%
C	4	1E-3	49.9%
D	5	1E-6	0.1%
E	8	1E-6	0.1%

Table IIb Propulsion Fault Minimal Cut Sets

Attitude Determination and Control Subsystem Fault

	Fault	Lower level fault or failure	Rating	Risk reduction or elimination measure(s)	Cat.
1	Orbit Pos. Fault	GPS receiver failure	4	Heritage; physical redundancy	II
2		GPS interface card failure	4	Heritage; physical redundancy	II
3	Att. Deter. Fault	Star Tracker failure (nc)	4	Heritage; second unit remains operational	III
4		1553 Bus Controller (Card) failure	4	Heritage; physical redundancy	II
5		Sun Sensor head failure (nc)	4	Heritage; fourteen (14) units total	II
6		SEP Amplifier Card failure	4	Heritage; SEP is internally redundant	II
7		Reaction Wheel failure	3	Heritage; fourth three-axis wheel available	II
8		Reaction Wheel Interface Card failure	4	Heritage; physical redundancy	II
9		Magnetometer failure	4	Heritage; physical redundancy	II
10		Magnetometer Interface Card failure	4	Heritage; physical redundancy	II
11		Solar Array Potentiometer failure	3	None specified	I
12		ADCS Control Console failure	4	Heritage; checkout/certification prior to use	I
13	Att. Cntrl Fault	Thruster Interface Card failure	4	Heritage; physical redundancy	II
14		SEP thruster driver failure	4	Heritage; SEP is internally redundant	II
15	Att. Cntrl Fault	Torque Rod failure	3	Heritage; physical redundancy	II
16		Torque Rod interface card failure	4	Heritage; physical redundancy	II
17		SEP Torque Rod driver failure	4	Heritage; SEP is internally redundant	II
18	Desire Att. Fault	Command build failure	3	Extensive ground verification and verification	IV
19		Command interpretation failure	4	Extensive ground verification of spacecraft	IV

Table IIIa Attitude Determination and Control Fault Risk Ratings and Fault Catagories

reduced knowledge and pointing accuracy.

"Level IV": A catastrophic fault rendering the system being analyzed as completely non-operational.

For Each Level IV Fault...

Since we are only interested in faults that would cause a potential failure to meet the nominal mission success criteria, only level IV faults need be examined further. The steps to be taken at this stage are as follows.

VI. Minimal Cut Sets – Identify "minimal cut sets", each one being an intersection of events (lowest level failure modes), and calculate the failure probability for each. In this case, the latter would simply require that each rough order of magnitude failure probability of a given cut set to be multiplied together.

VII. Rare Event Approximation – Use rare event approximation to calculate the failure probability at the subsystem level (i.e. the sum of minimal cut set probabilities).

VIII. Levels of Importance – Calculate the relative quantitative importance of each minimal cut set (i.e. the ratio of the minimal cut set failure probability and the sum).

IX. Focus Areas – Highlight minimal cut sets with the highest relative quantitative importance percentages, and focus reliability actions on these items.

	Minimal Cut Set	Probability	Importance
A	18	1E-3	90.0%
B	19	1E-4	10.0%

Table IIIb Attitude Determination and Control Fault Minimal Cut Sets

In order to gain a better understanding of the seven steps required to complete the probabilistic risk assessment, we'll turn our attention back to the three subsystem fault tree 'branches' examined earlier and then apply the defined series of activities on each one.

Risk ratings and fault categories for the negative power balance fault tree branch are shown in Table Ia. One can see that in almost all instances the lowest level events are either active mechanical or electrical failure modes, therefore, risk ratings are either 3 or 4. The next step is to list any and all fault reduction or elimination/retirement actions already taken. This way when fault categorization is done, the assessment can be done taking into consideration as many factors as possible. The failure modes that could potential result in a level IV catastrophic fault are the three active mechanical components in the solar array fault scenario and the battery charge/discharge failure. These four failure modes are defined as the "minimal cut sets". Table Ib shows the relative quantitative importance of each of these cut sets. From these percentage levels it is obvious that the three active mechanical failure modes in the solar array fault scenario are the ones that merit the most attention.

Risk ratings and fault categories for the propulsion fault tree branch are shown in Table IIa. One can see that active mechanical failure modes are contrasted by passive failure modes. Therefore, most risk ratings are either 3 or 6. The next step is to list any and all fault reduction or elimination/retirement actions already taken. The failure modes that could potential result in a level IV catastrophic fault are four of the five failure modes in the propulsion tank fault scenario and the structural integrity failure mode of the plumbing fault scenario. These five failure modes are defined as the "minimal cut sets". Table IIb shows the relative quantitative importance of each of these cut sets. From these percentage levels it is obvious that the two active mechanical failure modes, fill/drain valve and fill/vent valve, in the propulsion tank fault scenario are the ones that merit the most attention.

Risk ratings and fault categories for the attitude determination and control fault tree branch are shown in Table IIIa. One can see that most of the lowest level events are either active mechanical or electrical failure modes. Therefore, most risk ratings are either 3 or 4. The next step is to list any and all fault reduction or elimination/retirement actions already taken. Given the considerable amount of physical and functional redundancy in the attitude determination and control subsystem, most failure modes are categorized as only level II faults. Recall that these faults reduce overall system capacity, but do not degrade on-line performance. The only failure modes that could potential result in a level IV catastrophic fault are associated with a command build or interpretation failure mode. These two failure modes are defined as the "minimal cut sets". Table IIIb shows the relative quantitative importance of each of these cut sets. From these percentage levels it is the command build failure that merit the most attention.

5. CURRENT ASSESSMENT

The goal at the conclusion of project formulation phase was to have a preliminary version of the CloudSat system-level fault tree and the relativistic probabilistic risk assessment prepared. This would enable the team to identify residual risks and to reduce or eliminate/retire them through changes in design. After meeting the goal and completing an initial assessment the following conclusions were drawn.

Firstly, most failure mode risk ratings were determined to be either "3" or "4", one-in-one-thousand and one-in-ten-thousand probability of occurrence, indicating that most faults are active mechanical or electrical component potential failures.

Secondly, most spacecraft failure modes fell into the level II category, a fault reducing overall system capacity, but not impacting on-line performance, due to the extensive use of physical and functional redundancy.

Thirdly, based on minimal cut set levels of importance te focus should be on:

- Single-string components
- Components with little to no flight heritage
- (Human) error-prone processes (e.g. command generation

Fortunately, all three of these items were already identified as focus areas for the project team. Therefore, the added-value to date by completing the preliminary version of the CloudSat system-level fault tree and the relativistic probabilistic risk assessment is confirmation that the project team focusing attention in the proper areas.

Finally, there had been some discussion about the possibility of all NASA flight projects being required to use a standard software application or tool suite in preparing a fault tree and conducting a probabilistic risk assessment. In addition, the CloudSat team was also interested in knowing whether or not the streamlined process was valid or completely orthogonal to more traditional methods. After being informed about one such tool suite being considered – SAPHIRE (Systems Analysis Programs for Hands-On Integrated Reliability Evaluations) a request was made to obtain user manuals and demonstration software, so that a test case could be run and compared with the results of the CloudSat process. The negative power balance 'branch' was selected. After carefully inputting the fault tree and probabilities occurrence for each of the low-level failure modes into the software applications, the output showed that the results were very similar. For example, the minimal cut sets with the highest levels of importance were demonstrated to be within 3 percentage points of that resulting from the CloudSat process. The reason for this is clear. The SAPHIRE tool takes into consideration all of the failure modes identified in the fault tree, while the streamlined CloudSat process only considers those failures modes that could potential result in a level IV catastrophic failure.

6. FUTURE WORK

The commitment through project implementation phase is to construct the final CloudSat system-level fault tree and complete the final relativistic probabilistic risk assessment. Links to bottom-up analyses such as FMECAs and WCAs (Worst-Case Analyses) will also be demonstrated to ensure that an accurate and valid investigation was completed. The team would still attempt to identify residual risks, but the measures to reduce or eliminate/retire them would primarily be a result of contingency planning.

7. CONCLUSIONS

The CloudSat Project has taken to heart the NASA directive to augment the traditional risk management approach with fault tree analysis and probabilistic risk assessment. In order to comply with current budget and schedule constraints and still respond positively to the directive, a streamlined approach has been developed that will yield value-added results throughout the development life cycle. Initially, this will be used to assist with design improvements and later to assist with contingency planning.

To date, the results of the preliminary CloudSat Project fault tree analysis and probabilistic risk assessment have confirmed that the team is concentrating limited risk mitigation resources in the proper areas. However, final versions of each are to be prepared and made available at the critical design review, and future "as needed" revisions will be generated through the remainder of the development life cycle. Analyses will be made periodically, and these or may not necessarily result in the same assessment.

It is hoped that this streamlined approach will encourage other NASA flight projects to look at both fault tree analysis and probabilistic risk analysis as additional tools or methods to achieve mission success.

REFERENCES

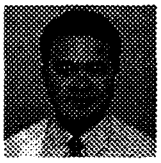
[1] Reliability Tool Kit: Commercial Practices Edition

[2] Guidelines for Program/Project Responsibilities for Safety and Mission Success, 2000. (http://www.hq.nasa.gov/office/codeq/sms.pdf)

[3] Fault Tree Handbook, U. S. Nuclear Regulatory Commission, NUREG-0492, January 1981.

ACKNOWLEDGEMENT

This work described in this publication was performed at the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California under contract with the National Aeronautics and Space Administration.



***Ralph R. Basilio** is the CloudSat Spacecraft Manager and serves as the contract technical manager for the Ball Aerospace & Technologies Corporation spacecraft system contract. He has twelve years of engineering and management experience working on space flight projects such as the Space Shuttle, and Galileo, Cassini, Mars Pathfinder, and Deep Space 1 Projects. He is a recipient of the NASA Exceptional Achievement Medal, over twelve NASA Group Achievement Awards, a JPL Group Award for Technical Excellence, and a JPL Level A Bonus Award for Outstanding Accomplishments. He is a graduate of the California Institute of Technology's Executive Engineering Management Program, and holds MS and BS Degrees in Aerospace Engineering from the University of Southern California (USC) and the California State Polytechnic University, respectively. He is pursuing further graduate studies in the USC Aerospace and Mechanical Engineering Department leading up to the Engineer and PhD degrees. He has authored/co-authored twelve technical papers, and served as the general co-chairman for a technology validation symposium.*

***Kim S. Plourde** is the CloudSat Mission Assurance Manage. Kim Plourde has over twenty years of experience in commercial and military/government electronics, to include automotive, ground, sea, airborne and space-based applications. He has worked in a variety of materials, EEE parts, reliability and quality engineering positions at Martin Marietta, Hughes Aircraft, Delco Electronics and Raytheon Corporation. Previous assignments include Product Assurance Manager at Hughes Santa Barbara Research Center, and Quality Director at Raytheon Systems Corporation.*

He earned his BS in Polymer Science at Pennsylvania State University, his MS in Management at Troy State University-European Division and his MS in Materials Engineering from California State University Northridge. He is also a graduate of the United States Air Force Air War College.

Try Lam *is an academic part-time employee pursuing a BS Degree in Aerospace Engineering at the California State Polytechnic University*