Fault Tree Analysis of the HERMES CubeSat

Felix Bidner
University of Colorado at Boulder
Adviser: Kendra Kilbride
bidner@colorado.edu
March 29, 2010

Abstract

Failure analysis plays an important role in the engineering design process, as failure events are expected and need to be accounted for in any design. One technique for evaluating the potential faults that may occur within the system is known as Fault Tree Analysis (FTA), a deductive method that takes an undesirable state in the system and works backwards to identify how it may have come about. The result is a logic tree that illustrates how certain faults, or combinations thereof, will lead to the undesired state. The visual nature of the FTA makes it effective in identifying the propagation of faults throughout the system; in turn, the vulnerable areas of the system can be determined and prioritized.

This paper presents an overview of the ongoing Fault Tree Analysis that is being performed on the HERMES CubeSat and offers the benefits that such an FTA presents for the mission.

1. Background

1.1. Introduction to FTA

Fault Tree Analysis (FTA) is an "analytical logic technique" that was developed at Bell Laboratories in 1962 to evaluate the Air Force's Minuteman ICBM Launch Control System. Shortly thereafter it was adopted for use with the Boeing Company and has since become commonplace throughout the aerospace industry.

FTA is a deductive approach where the first step is to identify an undesired event in the system; this becomes the "top event" of the fault tree. Then, the system is investigated to find all the possible ways that the undesired event could occur. Typically, any cause of the undesired event can be described as a sequence of small-scale faults in the system that, taken together, bring about the more critical top event. Such faults can be the result of a hardware or software malfunction, human error, or any other occurrence that will lead to the undesired state. The fault tree is then built up from these fault sequences, with each "branch" consisting of a particular sequence of fault events that will cause the top event to occur. The fault tree takes the form of a logic block diagram with Boolean logic gates connecting each event (an overview of FTA symbology will be provided in section 1.4). A basic example of the fault tree form is given in Figure 1 below.

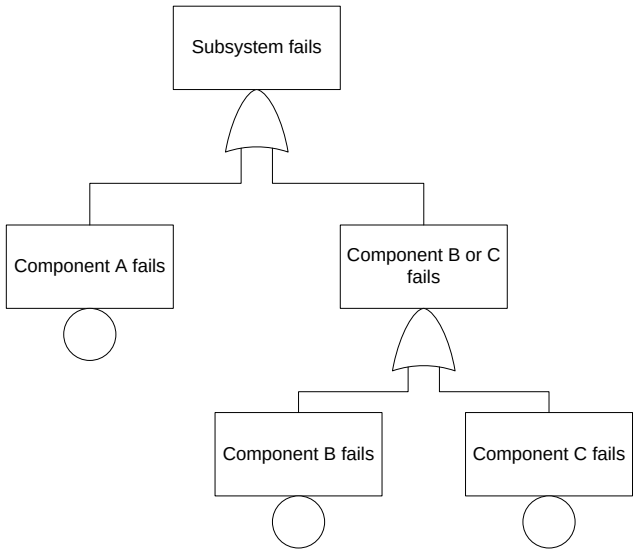


Figure 1: Sample fault tree diagram.

In the simplified fault tree of Figure 1, the subsystem will fail if one of the components A, B or C fails.

1.2. Why Use FTA?

FTA is one of many failure analysis methods in use in the aerospace field, and often it is complemented with another technique known as Failure Modes and Effects Analysis (FMEA). The difference between these methods is that FMEA is a bottom-up approach that identifies all of the possible failure modes of a single component in the system and lists the resulting consequences, whereas FTA is a top-down approach that begins with a system-level fault and works backwards to identify the root causes[1]. One of the main benefits of FTA is that it shows how various combinations of events can lead to a major undesired state, and furthermore, a fault tree can reveal relationships between events across different subsystems. Because individual parts of the system are usually designed by separate teams and integrated only after each part is completed, it can be difficult to predict how the parts will interact with one another once they are incorporated into a single system. Thus, identifying how the interactions between subsystems can lead to undesired events is one of the most powerful applications of FTA.

Another use of FTA is in systematically prioritizing, according to importance, the basic events that lead to the top event [1]. If the probability of the occurrence of each basic event can be predicted, then the overall probability of the sequence leading to the top event can be determined as well. This makes it possible to determine which fault events are the largest contributing factors to the top event, and consequently allows the user to allocate time and resources toward addressing the most influential events. In many cases, a select few basic events are the leading contributors to the undesired state, and identifying them allows for more focused and efficient action – whether that be addressing the issue in the design stage or figuring out how to deal with the problem once it has occurred.

This comes to the versatility of FTA in both revealing weaknesses in the design and in diagnosing fault events that have already occurred [1]. As a preventative tool, FTA can be used to recognize vulnerabilities in the system, which in turn can be corrected or improved before the undesired event takes place. Combined with the prioritizing process discussed earlier, the design can be improved in the most efficient manner possible. Meanwhile, if the design has already been completed and put into use, then FTA becomes an effective tool for pinpointing the causes of fault events that occur during operation. In this manner, it is possible to troubleshoot not only top events of an FTA, but also any intermediary events that occur (in other words, any event contained within a branch of the fault tree can be evaluated).

1.3. Performing a Fault Tree Analysis

When attempting to carry out a successful FTA, it is crucial to keep in mind the purpose behind the analysis, and this begins with clearly defining the objective of the FTA. The objective can be described as examining an event that will lead to mission failure and identifying all of the possible ways in which this event can come about. It is possible to have multiple objectives, which frequently occurs if the mission is divided into multiple phases – each phase may entail different mission objectives. The event given in the objective becomes the top event of the fault tree; there may be more than one top event (even for a single objective), in which case multiple fault trees will be constructed [1].

Next, the scope of the fault tree must be defined, which assigns limits to how in-depth the analysis will be. This is up to the judgment of the user but in most cases, the fault tree should be developed to a level at which the user can exert some control over the system. For example, when evaluating the potential failure of circuit components in a design, a potential cause may be faulty manufacturing of the component, but it would be unreasonable to delve any further into the nature of the manufacturing flaw. Additionally, boundaries must be assigned to the analysis to describe what parts of the system will be included and excluded from the FTA. It is impractical (and probably impossible) to include every aspect of the system in the analysis of a particular top event; hence, assumptions are made as to the state of those components that do not play a major role in the analysis [2]. For instance, when investigating structural weaknesses in a satellite it would likely be unnecessary to examine the power supply in detail, so typically we would define the power supply as

operating normally and exclude it from any further analysis.

Once the objective, top event, and scope have been established, construction of the fault tree becomes possible.

1.4. Fault Tree Symbology

The fault tree is composed from two fundamental components: event blocks and logic gates. Figure 2 shows the event symbols used in fault trees.

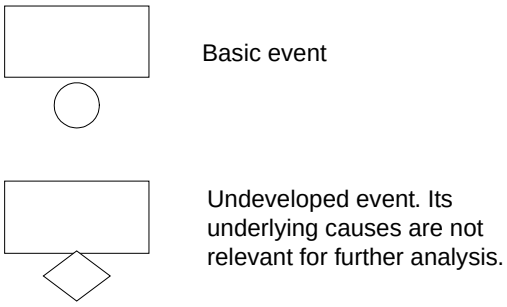


Figure 2: Fault tree event symbols [3].

An event is either followed by a gate or terminates as a basic or undeveloped event. The difference between basic and undeveloped events is somewhat arbitrary, as basic events are also due to underlying causes that we choose to ignore, but for clarity both types of event blocks are employed in practice.

Events in the fault tree are connected by logic gates as outlined in Figure 3.

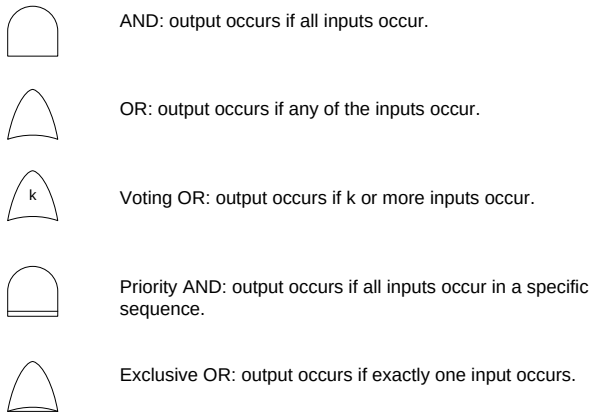


Figure 3: Fault tree gate symbols [3].

In practice, AND and OR gates are the most common gates utilized in FTA. One more symbol sometimes seen in FTA is the transfer symbol, represented by a triangle, which simply indicates that the continuation of that branch of the tree can be found on a separate page or section.

2. Application of FTA

2.1. HERMES CubeSat

An ongoing Fault Tree Analysis is being performed on the Hermes CubeSat to identify events that could lead to either partial or complete mission failure. While the CubeSat is still in the testing phase, the analysis is done from the standpoint that the satellite has been launched and is undertaking its mission.

For the initial stages of FTA, each of the subsystems of the HERMES was investigated separately. These subsystems were the ADCS, CDH, EPS (power), PCOM and HSCOM (primary and high-speed communications), Software, and the Structural and Thermal subsystems (Ground Station analysis has not yet been addressed). First, a top event was defined for a particular subsystem, such as insufficient power being supplied by the EPS. FMEA's of the subsystems had already been developed by their respective design teams, providing an exhaustive list of potential component failure modes and effects. The primary task in the FTA was to determine the relationships between components in a given subsystem and find how combinations of component faults could lead to the top event. In many cases, it took only one component fault to result in a top event – such events were classified as single points of failure, because if such an event occurred it would lead to potential failure of the entire system. An instance of such a failure would be if the batteries failed, which would lead to the satellite being powered only by the solar panels and thus incapable of operating when eclipsed by the Earth. One of the challenges was in fitting the information from the FMEA's into a fault tree model. In order to accomplish this, it was necessary to start with a failure listed in an FMEA and systematically work

backwards, with the expectation that the cause of the failure could also be obtained from the FMEA.

As explained earlier, one of the most powerful applications of FTA was to establish the relationships across subsystems, and this was the next step undertaken. One of the chosen top events was the loss of radio signal from the high speed communications system, HSCOM (see Appendix A for the corresponding fault tree). Some of the events that could lead to this condition were faults within the HSCOM subsystem itself, affecting components such as the radio or the modem. These events were contained to the subsystem and were straightforward. However, other causes were due to faults in other subsystems: the antenna may be pointing towards ground inaccurately, which is an ADCS issue, or there may be insufficient power provided to the subsystem, which originates with the EPS. Note the use of transfer symbols to reference the ADCS and EPS fault trees (Figure 4 and Appendix B). Also, in the case of most basic or undeveloped events, a Y or N was assigned to denote whether the event was a single point of failure.

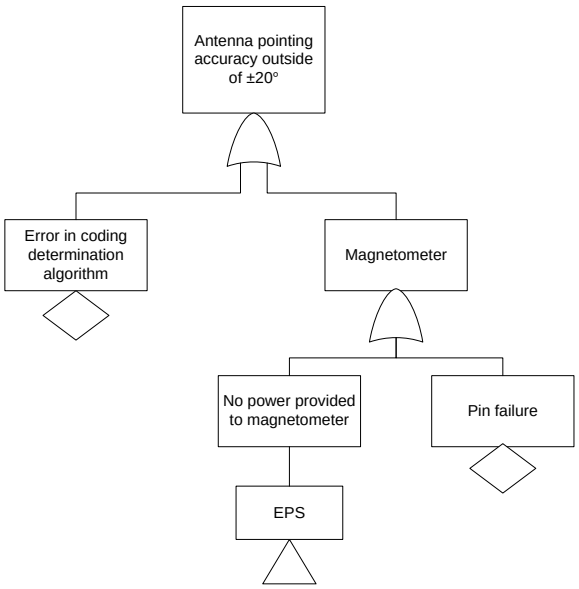


Figure 4: ADCS fault tree.

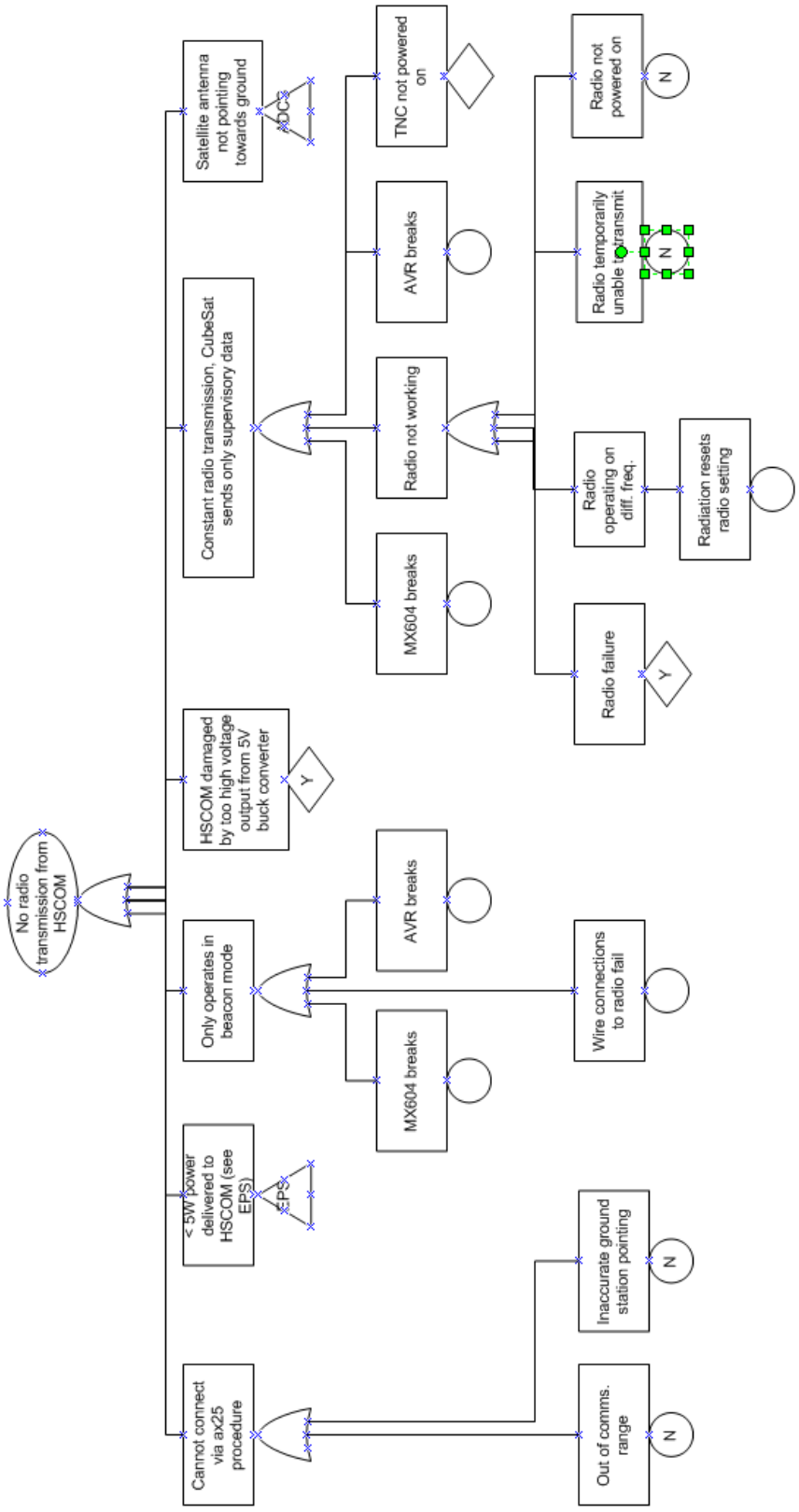
2.2. Refining the FTA

The fault trees provided in this paper are a sample of the analysis that has been performed on all of the CubeSat's major subsystems. With the exception of the Structural and Thermal subsystems, at least one top event has been defined for each subsystem and a fault tree is being developed for each of those events. (Most of these have been omitted here for the sake of brevity and readability.)

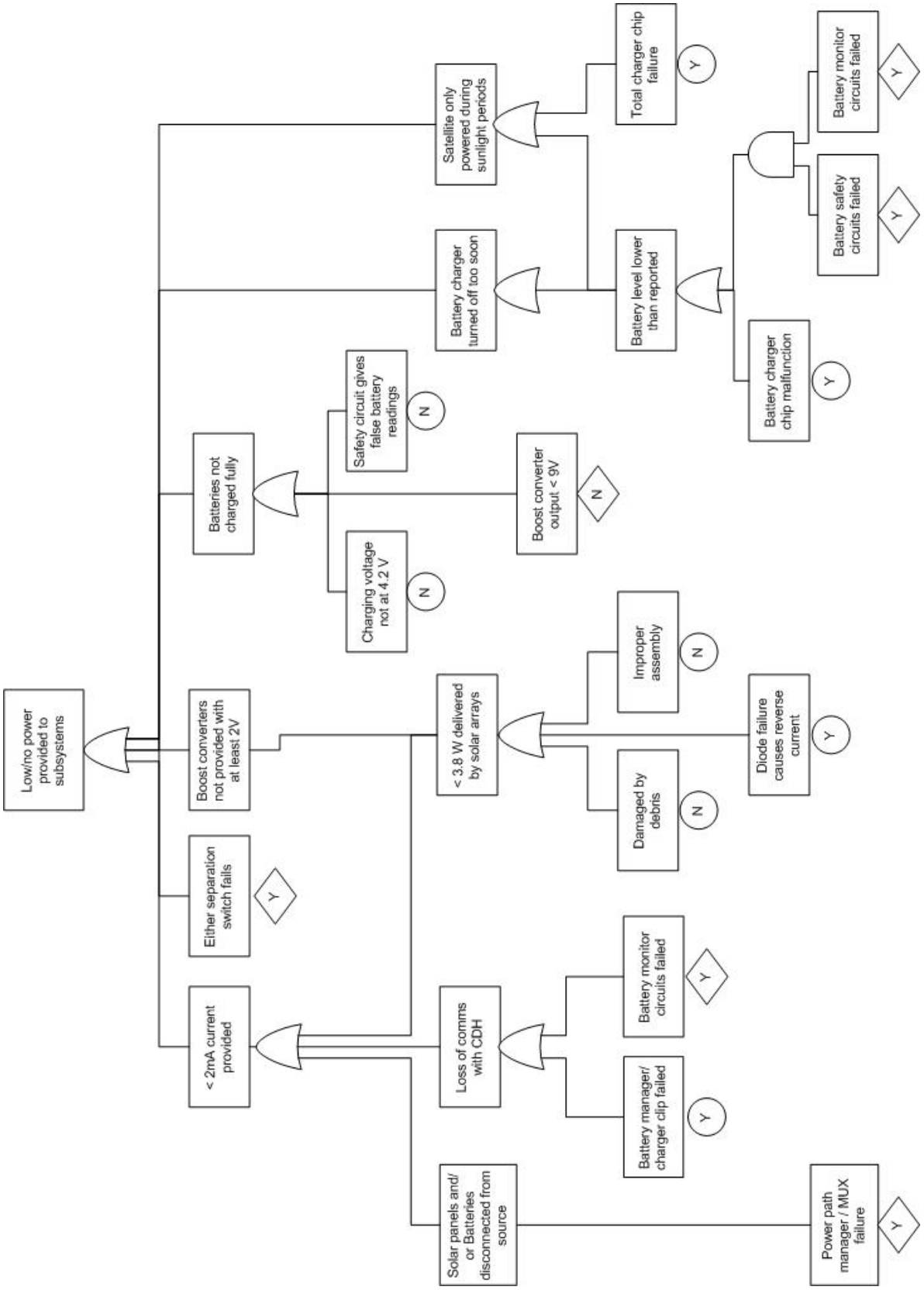
So far in this discussion of potential faults and failures in the system, the methods by which those faults are *detected* have been taken for granted. It may initially seem obvious, but there must be some form of data informing us of a malfunction. In the case of the CubeSat, its health and status are continuously monitored via onboard sensors and reported back to the mission operators. Current and voltage sensor readings must fall within an acceptable range that ensures the proper functioning of all onboard components. Consequently, it is extremely helpful to know how the sensors correlate to the components, so in the case of an anomalous reading it is easy to determine its cause. Work is being done to incorporate the proper sensor telemetry into the FTA, with each event correlating to a specified sensor value. This will greatly improve the FTA as a diagnostic tool for identifying faults and failures if they occur.

Finally, the current fault trees are being "quantified" to an extent. From the FMEA's, qualitative probabilities have been assigned to each event, ranging from "frequent" to "remote." Using this information it is possible to determine the probability of any particular fault tree branch to occur. While this is not a rigorous approach, it should help to intuitively describe which event sequences have the highest chance of happening.

Appendix A: HSCOM Fault Tree



Appendix B: EPS Fault Tree



References

[1] Stamatelatos, Michael, and William Vesely. *Fault Tree Handbook with Aerospace Applications*. NASA, Aug. 2002. Web. 29 Mar. 2010. <http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf>.

[2] Long, Allen R. *Beauty and the Beast - Use and Abuse of the Fault Tree as a Tool*. Tech. Fault-tree.net. Web. 29 Mar. 2010. <http://www.fault-tree.net/papers/long-beauty-and-beast.pdf>.

[3] "Fault Tree Analysis (FTA, System Analysis) Basics." *Reliability Engineering, Reliability Theory and Reliability Data Analysis and Modeling Resources for Reliability Engineers*. Weibull.com. Web. 29 Mar. 2010.