

Accident Investigation Using EEFTA
Clifton A. Ericson II
The Boeing Company; Seattle, Washington

Abstract

Fault Tree Analysis (FTA) is normally a proactive analysis tool for predicting potential causes of undesired events during the design of a new system. It is also a reactive analysis tool for ferreting out the root causes leading to an undesired event, anomaly, incident or accident that has actually occurred. FTA is very powerful as a structured methodology for identifying root causes, plus it also provides a visual communication model that most individuals can readily understand and follow with little knowledge of the tool, the system design or the accident situation. The visual model displays the logical progression in the chain of events leading to an anomaly or accident

This paper describes a modified Fault Tree technique referred to as *Evidence Event Fault Tree Analysis* (EEFTA) for analyzing accidents. The purpose of EEFTA is to reconstruct the actual events and conditions leading to an accident. Once the root causes are known, similar future accidents can be prevented through design changes. EEFTA facilitates rapid accident investigation to quickly establish the accident root causes without spending valuable time in unproductive non-causal areas. Also, root cause analysis is sometimes required in real time, in order to correct and prevent an anomaly from further progressing into a full-blown accident.

Overview

The *Evidence Event Fault Tree* is a standard Fault Tree utilizing a new gate type called an *Evidence Gate*. The Evidence Gate (EG) is similar to a check valve, in that it is either open or closed based on input conditions. In this case the EG either opens or closes a fault tree branch based on the collected empirical evidence. Evidence can be derived from many different sources, such as instrumentation data, witnesses, flight data recorder, video cameras, built in tests, etc. When a branch can be closed due to hard evidence, no further investigation is necessary in that particular area. Only the true root cause branches with supporting evidence are followed. In addition, branches with insufficient evidence

must be followed until either positive or negative evidence is found, or the root causes are identified. For example, an undesired state in a fault tree might be *Tank Over Pressurization*, but after review of available evidential data it was found that the tank's relief valves were working properly, thereby eliminating this path as a contributor to the incident.

In highly complex systems, not all safety problems can be completely identified and eliminated during the design of the system. Occasionally a few potential hazards fall through the identification crack, and can only be discovered when they actually occur during system operation. This is due to the fact that system complexity becomes too large for human comprehension to completely foresee all possible potential hazards or accidents. Therefore, when an anomaly or accident does occur, Reactive FTA is a valuable tool for analyzing and modeling the incident.

FTA can only be performed on an actual or suspected hazard in order to identify the root causes of the hazard. If the hazard is not known or suspected, then a FTA cannot be performed. FTA is primarily performed during the design phase, in order to identify critical weak links in the design, which are then mitigated to prevent their occurrence. An example of this situation occurred on the B-1A bomb bay doors. Hazard analyses identified the Undesired Events (hazards) of "Inadvertent Operation", "Failure to Operate Correctly" and "Premature Closure". These potential hazards were foreseen and could be evaluated by FTA. However, the potential hazard of "Bay Door Close Command Remains ON Continuously" was not foreseen as a hazard, until it actually occurred during a maintenance operation, nearly causing injury to the maintenance personnel. This type of incident results in a Reactive FTA, because the hazard was not foreseen during design, and therefore not investigated and mitigated.

One of the strengths of EEFTA is that it provides an approach to organize accident speculation in a structured graphical manner. Fault events, paths, conditions and relationships are displayed in a standardized graphical notation that is very easy

to understand and follow. The model can be easily modified as more data and information becomes available. This model also provides clues as to where and what type of evidence is needed by the investigators.

In an accident investigation there are two basic goals, (1) to *quickly* find the root cause(s) and (2) to *effectively utilize factual data* to help identify the root cause(s). EEFTA satisfies both of these objectives. It provides a methodology for incorporating evidence into both the analysis and the model. It also indicates where evidence is needed in order to make a decision regarding root causes. At the same time, the evidence closes analysis effort on paths that did not cause the incident. These paths can be re-opened at a later time if necessary.

Accident Investigation

What is accident investigation? The standard definition is analysis and evaluation of an accident to determine the specific root cause or causes of the accident. The intent is to determine product or process defect, in order that changes can be implemented to prevent any similar accidents. Quite often the conditions and events leading to an accident can be very complex. Much detective work is necessary to combine all of the clues, information and hard evidence leading to a final conclusion.

Accident investigation is akin to performing a system autopsy. It carefully considers all possible conditions and paths leading to the root cause(s) of the accident. The analysis follows given clues down the correct path, and documents the entire analysis process in a pictorial model that can be followed by other analysts.

FTA is an excellent tool for analyzing a design or an accident and identifying and modeling the root causes. When conducting an accident investigation it is often necessary to establish the root causes as quickly as possible. The EEFTA approach facilitates rapid accident investigation to quickly and correctly identify root causes, without wasting analysis time in areas that do not actually contribute to the accident. It provides a notation for the inclusion of evidence either supporting or negating a particular suspected causal event or branch.

If the evidence supports a fault path hypothesis, then that path is followed further until either the root causes are located, or another EG shows why that path is not the root cause. If there is insufficient evidence to draw a conclusion, then the path must be followed.

There are several different perceptions of accidents, and differing views regarding the root causes of accidents. The varying accident perceptions fall into the following categories [ref. 1]:

- 1) Single Event Perception
Treats the accident as a single event (generally a scapegoat).
- 2) Chain of Events Perception
Treats the accident as a chain of sequential events, like a domino effect. Investigators look for information that will permit reconstruction of the chain of events. The search focuses on unsafe events, conditions and causes.
- 3) Determinant Variable Perception
Treats the accident as dependent upon a single independent variable. The search focuses on the single independent variable. The goal is to gather data in a way that statistical comparisons will permit fair estimations on the independent variable and the probability of it causing the accident, given the factors and conditions are present.
- 4) Logic Tree Perception
Treats the accident as a converging chain of events leading to the accident. The events can occur in various sequential and/or parallel paths. This perception falls along the lines of FTA and EEFTA.
- 5) Multilinear Events Sequence Perception
Treats the accident as a segment of a continuum of activities. The accident process can be described in terms of specific interacting actors, each acting in sequential order with discrete temporal and spatial logical relationships (ie, timelines).

The Evidence Gate

The Evidence Gate (EG) is similar to a check valve, it is either open or closed depending upon the input conditions. The EG opens a tree branch when there is evidence to support it, or lack of evidence sufficient to make a judgment, and it closes a tree branch when there is sufficient evidence to support that conclusion.

When evidence is available to show that a particular branch did not happen, then that branch is ruled out, and no further analysis need progress down that path. If there is no evidence, or positive evidence supporting a path, then this indicates the direction the analysis should follow. The model shows what was considered and ruled out, and why certain paths were followed, hopefully to the actual root causes. The model considers all possible contributors - hardware failures, software errors, personnel errors, environmental factors, procedure errors, etc.

The overall purpose is not to quantify the probability of the incident, but to identify and model the events and conditions leading to the incident. In effect, its purpose is as a root cause identification tool, and as a model of the root cause relationships. Since the accident has already occurred, probabilities are generally moot at this point. Causal factors include hardware failures, software errors, human errors, procedural problems, environmental contributors and abnormal conditions.

Figure 1 shows the structure of the Evidence gate. As depicted by this example, the evidence condition is attached to the right side of the gate. The collected empirical evidence is placed inside this conditional event node. The evidence supports the output node either positively or negatively. If the conditional event node is true the analysis continues, if false the analysis stops at that point. Occasionally a fault tree will be developed either independent of the evidential data, or it may be developed faster than the data is collected. In these cases the FTA may go past the point where evidence would terminate a branch. The FTA is also instrumental in guiding the investigation in terms of where and what evidential data is needed.

Figure 2 depicts the methodology of the Evidence Gate for three different conditions. In the first case the tree branch is terminated with no further analysis because the evidence indicates that this hypothesized event did not occur. In the second case the branch was continued because there was evidence supporting the occurrence of events in this branch. In the third case the branch was continued because there was no evidence available to prove or disprove the considered event, thereby forcing continued analysis until evidence is found or the root cause is found.

Figure 3a depicts the overall structure of a large Proactive Fault Tree developed during the product design phase. Figure 3b depicts the general structure of a Reactive Fault Tree developed during an accident investigation analysis. Note that the Reactive Fault Tree structure tends to be smaller and more pruned (more shallow) than the Proactive Fault Tree. This is because the accident analysis fault tree is only after those particular events causing the accident or incident, whereas the Proactive FTA fully develops all causes and paths leading to the Undesired Event.

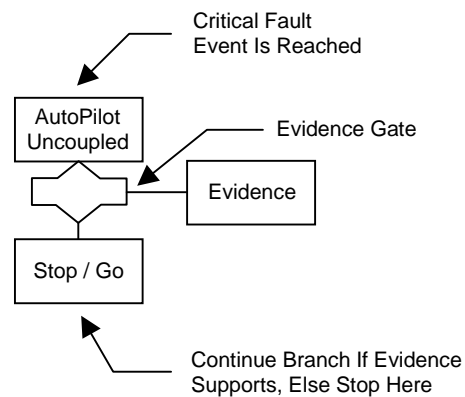


Figure 1 – Evidence Gate Structure

The methodology for developing an accident investigation fault tree is very similar to normal fault tree construction. There are two major steps involved:

- 1) First Pass Tree – Analyze system and incident using normal FTA construction rules and system logic. Identify and establish major system fault states that could possibly lead to the accident.
- 2) Second Pass Tree – Go through the first tree and determine where known evidence applies, or where additional evidence is needed. Place these conditions in the FT using the Evidence Gate. Continue down branches with positive evidence or insufficient evidence. Terminate branches with negative evidence.

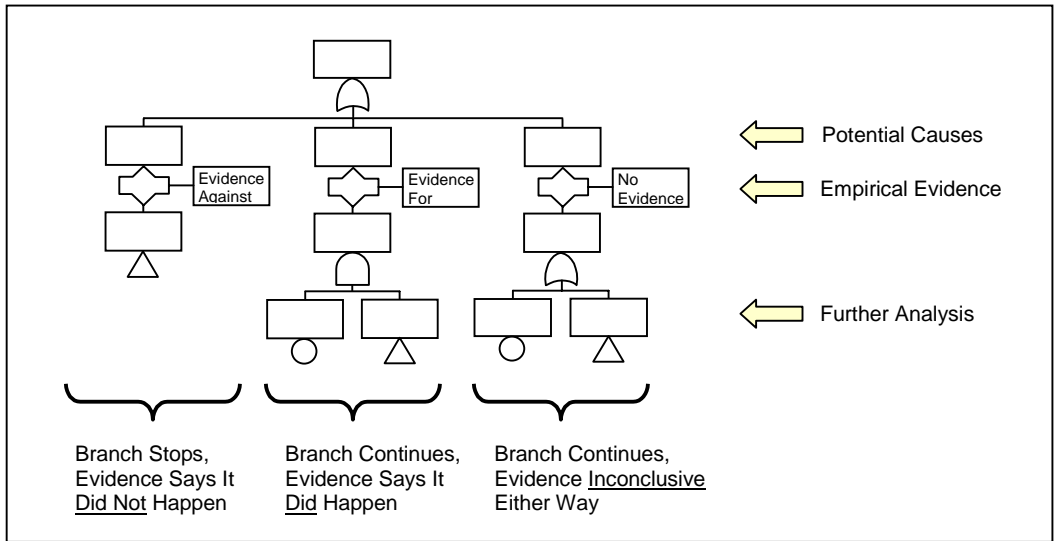


Figure 2 – Evidence Gate Methodology

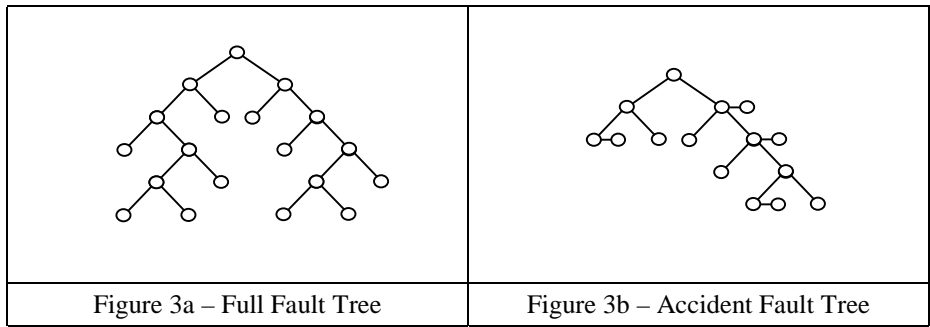


Figure 3a – Full Fault Tree

Figure 3b – Accident Fault Tree

Fault tree construction includes normal considerations, such as defining the system, which can be anything from a lawn mower to an aircraft carrier. Also, correctly defining the top Undesired Event is crucial in FTA and accident investigation.

Examples

Figure 4 is a photo of the recent aircraft accident that occurred at the Burbank, California, airport. In this accident the aircraft overran the runway, went through a barrier, crossed a busy street, hit one car and stopped just short of hitting a gas station. The EEFTA was conducted solely from information contained in Aviation News and Space Technology magazine [ref. 3]. Figure 5 (and 8) is an example EEFTA for this accident. The final tree branches were terminated due to lack of sufficient detailed information.

Figures 7 (and 9) are fault trees of the Titanic accident. The EEFTA was conducted from various news items containing information on the sinking of the Titanic [ref. 4]. This EEFTA attempts to show how analysis of this accident could be modeled.

Conclusion

The Fault Tree, utilizing the Evidence Gate, provides a complete cause-consequence root cause analysis diagram of the accident or incident under investigation. The Evidence Gate allows the user to insert actual evidence into fault tree branches, and thereby infer which events were active during an incident. This also allows the analyst to quickly home in on actual root causes, and not spend time analyzing possible scenarios that did not actually cause the

accident. It also provides a visual model, and list of all scenarios considered, and why some scenarios were ruled out due to specific evidence.

It should be noted that accident investigation fault trees tend to typically have more AND gates than do design phase fault trees. This is because the analysis and FT is not following every possible cause, as in a proactive FT, but only selective branches after they have happened. There are several possible explanations for this:

- 1) These types of fault trees trace only root cause paths leading to the event, while ignoring additional paths not involved.
- 2) An AND gate might be used to show inter dependent causes that could possibly be otherwise shown sequentially with OR gates.
- 3) Shows that accidents do often result from the cascading effect of multiple contributing cause factors.

Whether or not an EEFTA tends to have more AND or OR gates probably depends upon the complexity of the accident and the system involved. A large aircraft accident will likely have a lot of AND gates, whereas a small chemical process accident will likely tend to have more OR gates.

Quite often during an accident investigation it is very helpful (perhaps even critical) to draw upon the expertise of technical experts in different areas of the system. This assistance is for both correctness and timeliness. One of the strengths of fault tree analysis is that it allows experts with skills in different areas to individually contribute in their respective areas of expertise as the fault tree grows and expands. And, as the tree expands it also provides clues as to additional potential fault paths to consider.

Sometimes anomalies must be investigated in real time, in order that they can be resolved before the anomaly escalates into a major accident. EEFTA helps the analyst to quickly solve the problem by continually narrowing the scope of coverage through the use of Evidence Gates.

References

- [1] C. A. Ericson II, Fault Tree Analysis By Design, 16th International System Safety Conference, 1998.
- [2] Ludwiq Benner Jr., 5 Accident Perceptions: Their Implications for Accident Investigators, Hazard Prevention Journal, Sep/Oct 1980, Vol 16 No 11.
- [3] Aviation Week & Space Technology, March 13, 2000, page 40.
- [4] John Lancaster, Engineering Catastrophes: Cause and Effects of Major Designs, Abington Press, Cambridge, England, 1996, Chapter 2.

Biography

Clifton A. Ericson II
The Boeing Company
18247 150th Ave SE
Renton, WA 98058 USA

phone 253-657-5245
fax 253-657-2585
email: clifton.a.ericson@boeing.com
cliftonericson@cs.com

Mr. Ericson works in System Safety Engineering on Boeing AWACS programs. He has 34 years experience in system safety and software design with the Boeing Company. He has been involved in all aspects of fault tree development since 1965, including analysis, computation, multi-phase simulation, plotting, documentation, training and programming. He has performed Fault Tree Analysis on Minuteman, SRAM, ALCM, Apollo, Morgantown Personal Rapid Transit, B-1, AWACS and 737/757/767 systems. He is the developer of the MPTREE, SAF and FTAB fault tree computer programs. In 1975 he helped start the software safety discipline, and has written papers on software safety and taught software safety at the University of Washington. Mr. Ericson holds a BSEE from the University of Washington and an MBA from Seattle University. He is currently Executive Vice President of the System Safety Society, and is on the technical review committee for the Journal of System Safety and the Journal of Process Mechanical Engineering (UK).



Figure 4 – Aircraft Runway Overrun Accident

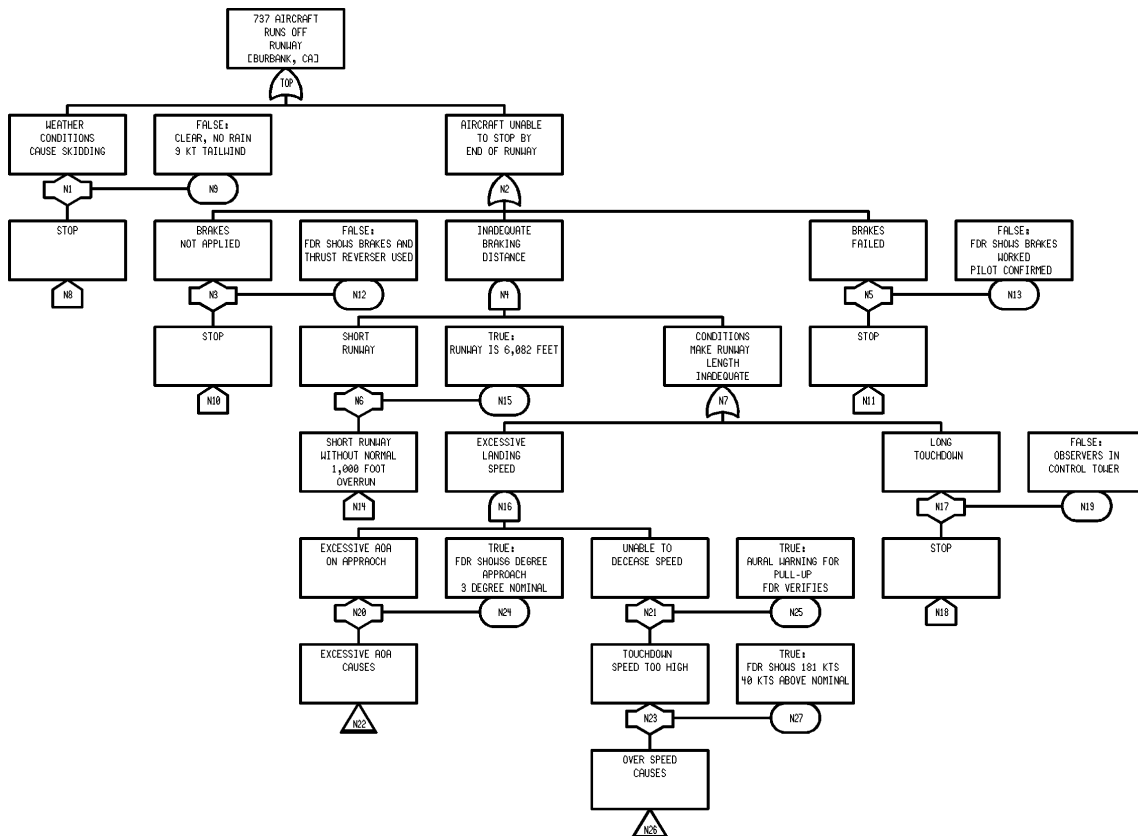


Figure 5 – Aircraft Runway Overrun Accident EEFTA



Figure 6 – Titanic Accident

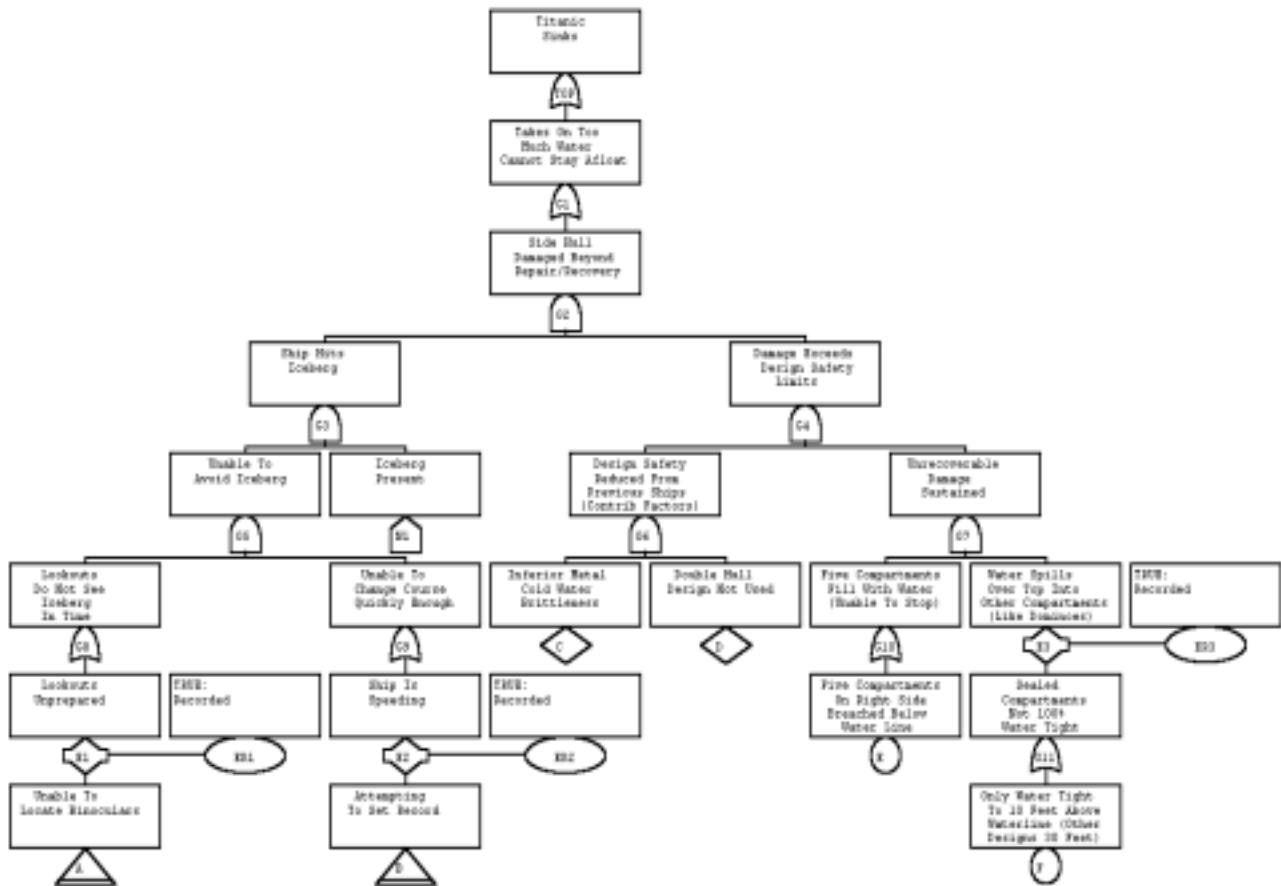
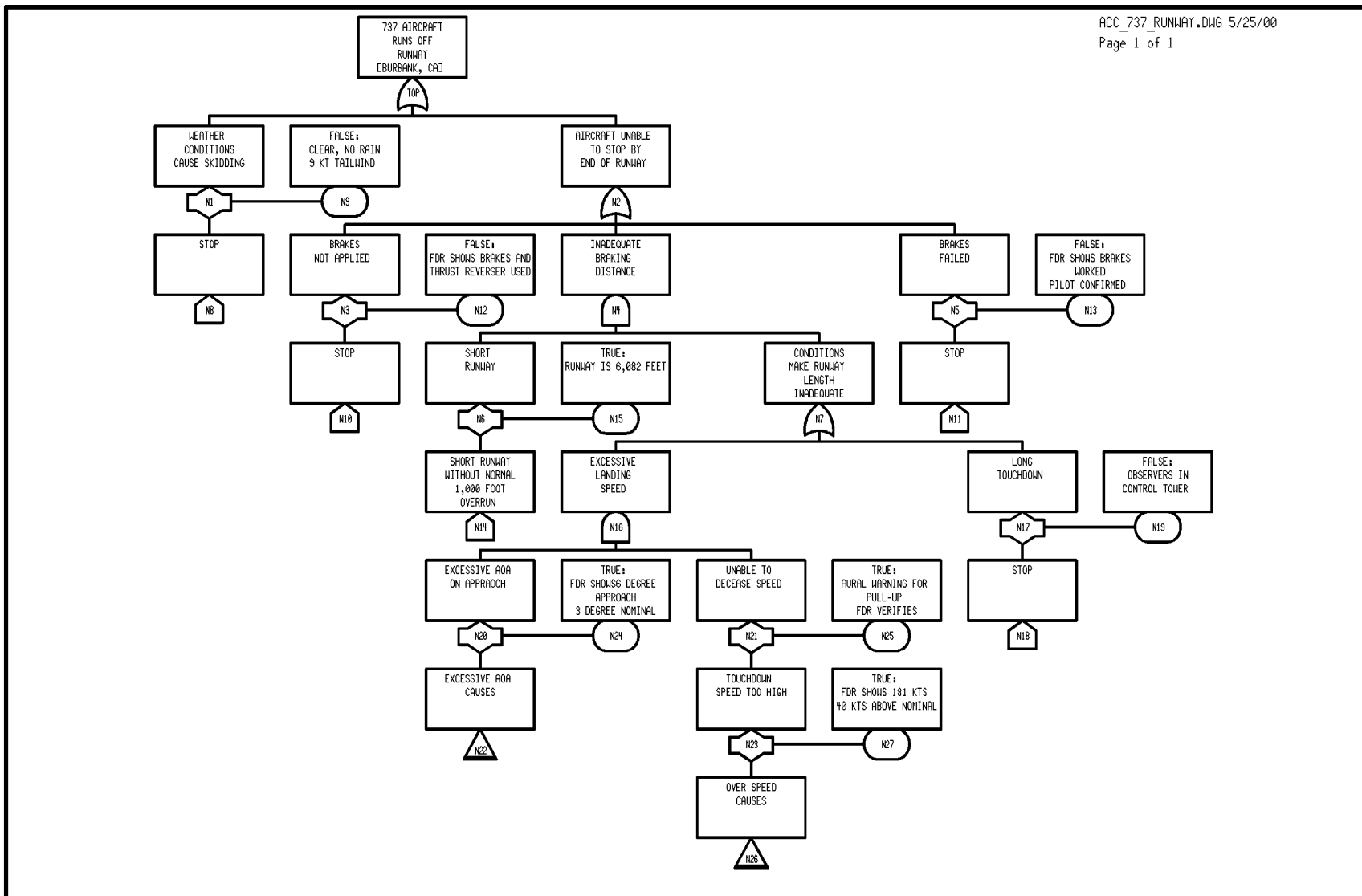


Figure 7 – Titanic Accident EEFTA



1. Reference - AIA&ST, March 13, 2000, page 40.
2. Southwest Airlines Flight 1455, Las Vegas to Burbank.
3. AOA - angle of attack.
4. FDR - Flight Data Recorder.

	INITIALS	DATE	MODEL	FTA Assoc.
CALC			737 AIRCRAFT RUNS OFF RUNWAY [BURBANK, CA]	Accident Investigation Evidence Event Tree C.A. Ericson
CHECK				
APPD				
APPD				
			TOP	

Figure 8 – Aircraft Runway Overrun Accident EEFTA

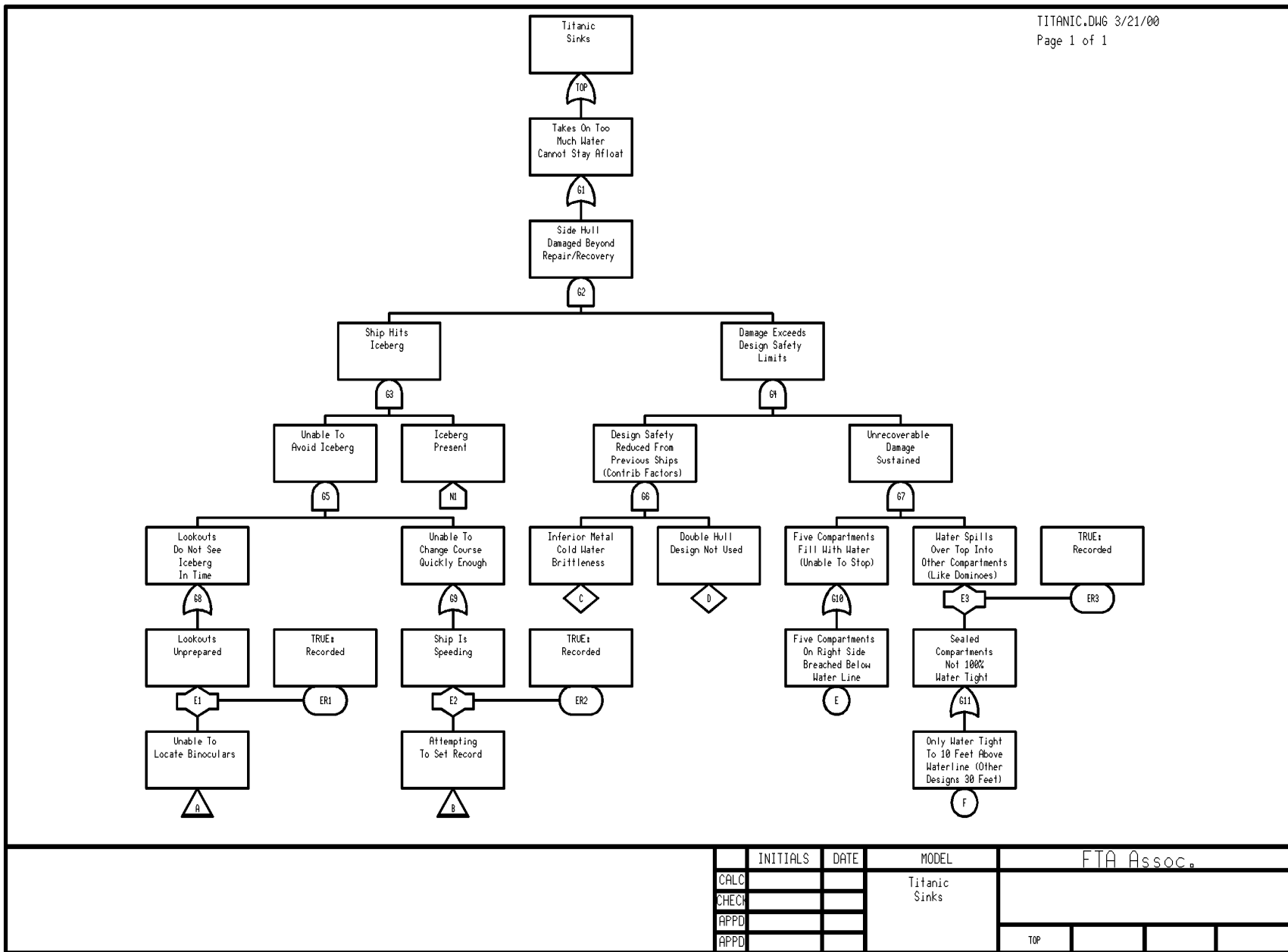


Figure 9 – Titanic Accident EEFTA