

Case Study – Use of FaultTree+ in a General Aviation Aircraft Reliability Study

Introduction

The case study is an example of the use of FaultTree+ in the Aircraft industry.

FaultTree+ is the world's most popular fault tree software package incorporating fault tree analysis, event tree analysis and Markov analysis. It can efficiently solve fault trees of 20,000 gates and 20,000 basic events, using world-class analytical methods. On top of this, the user-friendly interface (running in a standard Microsoft Windows environment) allows simple creation or adaptation of projects.

This document describes many of the useful features in FaultTree+ used in the construction of this fault tree. It also describes the variety of results provided by the software tool (minimal cut sets, importance rankings etc) and the variety of methods for extracting the data to other external applications and documents (Report Generator, import/export capabilities).

Study Description

The Advanced General Aviation Transport Experiment (AGATE) program is a government-university-industry consortium formed with the goal of developing technologies to revitalise the United States' general aviation (GA) industry. The program aims to make GA aircraft accessible to the general population. This will require aircraft that are both reliable and simple to operate.

In order to reach the required level of reliability, the baseline reliability of the cockpit instrumentation of GA aircraft currently in service must be determined. For the purposes of this report the instruments in question were grouped into the following six categories:

- Airspeed information
- Altitude information
- Attitude information
- Advisory panel (aircraft status information)
- Communications information
- Navigation information

This report reflects the probability that the above information is provided for the duration of a 700 nautical mile (NM), 6-hour flight.

For the purposes of the analysis the following major assumptions were made:

- Human factors were not considered
- The aircraft analysed was representative of the GA aircraft population
- External cues were not considered (e.g. Looking out of a window)
- The criticality of information was not considered

- All ground based navigation aids were available
- All components exhibit an exponential time to failure distribution
- Environmental elements were not considered
- Partial failures were not considered
- Out of tolerance conditions were considered as failures

The data used in the analysis was difficult to obtain partly due to propriety concerns among commercial providers, but mainly because there is no central clearing house for the retention of such information. GA aircraft instrumentation is maintained and repaired by many facilities worldwide.

The reliability information for this analysis was gathered from aircraft manufacturers and GA maintenance personnel. Information was also provided by a commercial delivery company operating single-engine cargo aircraft.

A simple mission profile of start-up to shutdown was considered, with normal operating procedures requiring power to all instruments for the duration of the flight time. The flight distance was 700 NM at an average air speed of 120 knots, giving a flight time of 5.86 hours. If pre- and post-flight taxiing is included the flight time increases to 6 hours.

The assumption that all time to failure data follows an exponential distribution is critical. This failure behaviour is common for electrical components, but could introduce inaccuracies if applied to mechanical components. With more detailed failure data for the mechanical systems, a simulation could be used to improve accuracy.

TOP Event Definition

The first step in any Risk Assessment is to identify the hazard/system failure of interest. This becomes the Top event of our Fault Tree. In this study, the Top event of interest is “Loss of cockpit instrumentation information.” The Top event occurs whenever at least one cockpit instrument fails or the information it provides is lost. Cockpit information may be lost either by the immediate failure of an instrument (altimeter, tachometer etc) or by the loss of power to the cockpit (alternator).

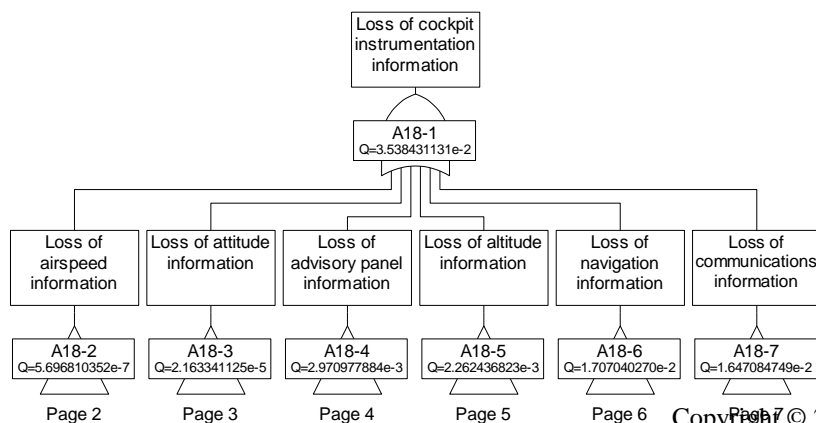


Figure1 – Top event and immediate inputs

Fault Tree Analysis

The analysis of the cockpit instrumentation involves these steps:

1. Building the fault tree model
2. Entering failure and repair parameters
3. Determination of minimal cut sets and quantitative parameters
4. Evaluating critical components
5. Reporting

The fault tree method involves the creation of a fault tree diagram composed of gates and basic events that represents the logical description of a system failure, known as the TOP event, in terms of the failure of the components that comprise the system. After creating the diagram, the user assigns failure characteristics of the system components. On completion of the model, the system analysis is performed. To do this, the FaultTree+ software first determines the minimum combinations of component failures that will cause a system failure. These are known as the minimal cut sets. Finally, FaultTree+ calculates the quantitative parameters such as system unavailability and failure frequency.

Building the fault tree model

A fault tree can be used to model the failure logic for the cockpit instrumentation TOP event. The loss of cockpit information can result from a single instrument failure, an appropriate combination of instrumentation failures, or from loss of power due to the failure of the alternator.

FaultTree+ provides an easy to use interface for constructing fault tree diagrams. The user simply adds gates and events by selecting an existing gate and dropping the new gate or event on to the selected gate. After creation, the new gate or event may be selected and its parameters modified. Extensive copy and paste facilities make the re-use of existing fault tree sub-trees an easy task. In addition to the diagram construction area, a spreadsheet is available for rapid access to and modification of gate and event parameters. Automatic paging facilities exist. Simply identify gates or branches with a new page tag and the program takes care of the pagination.

Appendix B contains a detailed fault tree of the hazard under investigation for the cockpit instrumentation.

Other features exist within FaultTree+ to facilitate the construction and analysis of complex fault trees. The append feature was of particular use at the construction stage. Smaller fault tree files developed by individual members of the Risk Assessment team can be appended to one another, with links being made at identically named gates. This allows the example file to be constructed initially as a large number of smaller, more manageable files. Then these are later appended to the master file containing the Top event.

The example file contains a number of events, each affecting an instrument in the cockpit. As well as applying failure data to each event manually, FaultTree+ allows the user to define generic failure models, each of which may be allocated to multiple events. The data for these models may be entered by the user or imported from a library.

Entering failure and repair parameters

The FaultTree+ “Edit Event” Dialog allows the user to select the event failure model, name and description.

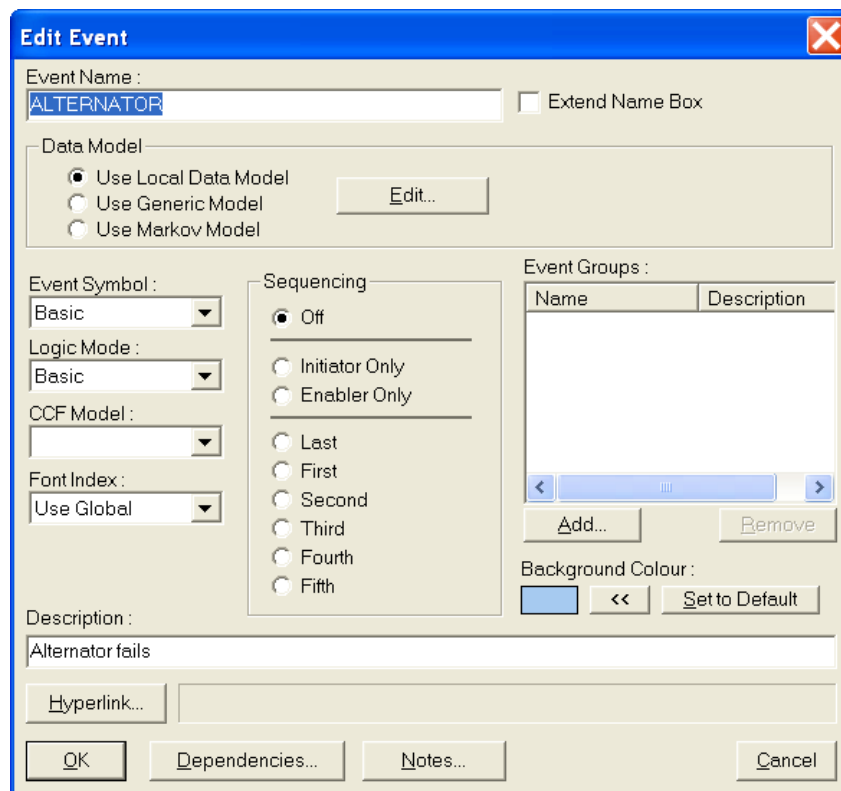


Figure 2 – Sample “Edit Event” dialog

Event features include:

- Select from failure model type
- Enter name and description
- Select a CCF model
- Select Logic Mode if True/False logic is applicable
- Select background color (if default is not wanted)

- Add the event to an event group
- Set the sequence of event failures
- Select a generic failure model. These are created by the user and may be applied to any basic event
- Enter notes and hyperlinks

Analysis

Verification checks provide diagnostic information before commencing an analysis and will help you to identify any errors in your models due to circular logic, undefined gates and invalid initiators.

The FaultTree+ program can calculate the cut sets for the system TOP event, as well as intermediate gates within the system. For this reason, the FaultTree+ contains algorithms to efficiently analyze a large fault tree. These algorithms include the ability to modularize the fault tree by breaking it apart and solving it in smaller, more manageable independent chunks. These simplifications are carried out in such a way that no information is lost for the common cause failure analysis. The minimal cut sets range in size from single-event cut sets to much larger cut sets. These cut sets enable us to see what combinations of failures will result in system failure and also to help pinpoint weaknesses in the system.

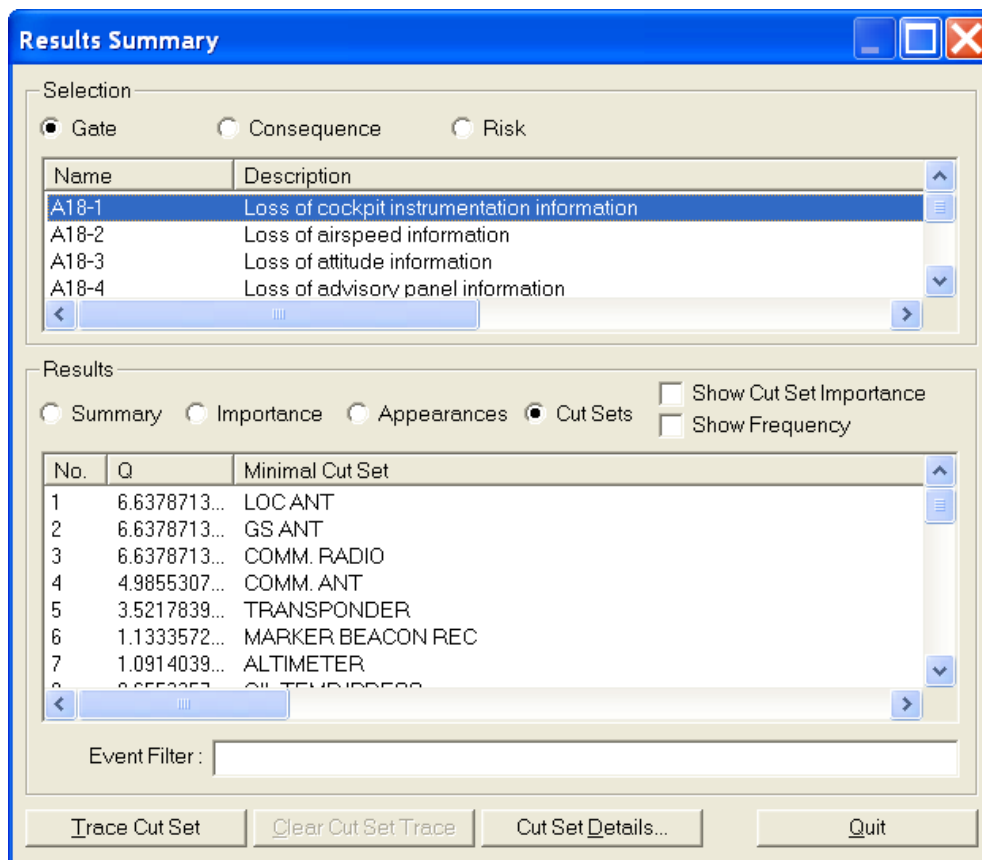


Figure 3 – Results Summary showing minimal cut-sets

The Partial Analysis feature of FaultTree+ gives the user the ability to analyze only the segment of the fault tree below a selected gate. This feature saves time at the testing stage by negating the need to run the analysis for the entire fault tree when they wish to check the minimal cut sets for only the part of the tree that they are currently working on.

Evaluating critical components

Importance measures are provided for both events and event groups. These help with the identification of critical failures and events where the accuracy of the failure and repair data is key. Sensitivity analysis allows the automatic variation of event failure and repair data between specified limits. Uncertainty analysis allows confidence levels to be determined from event failure and repair data uncertainties.

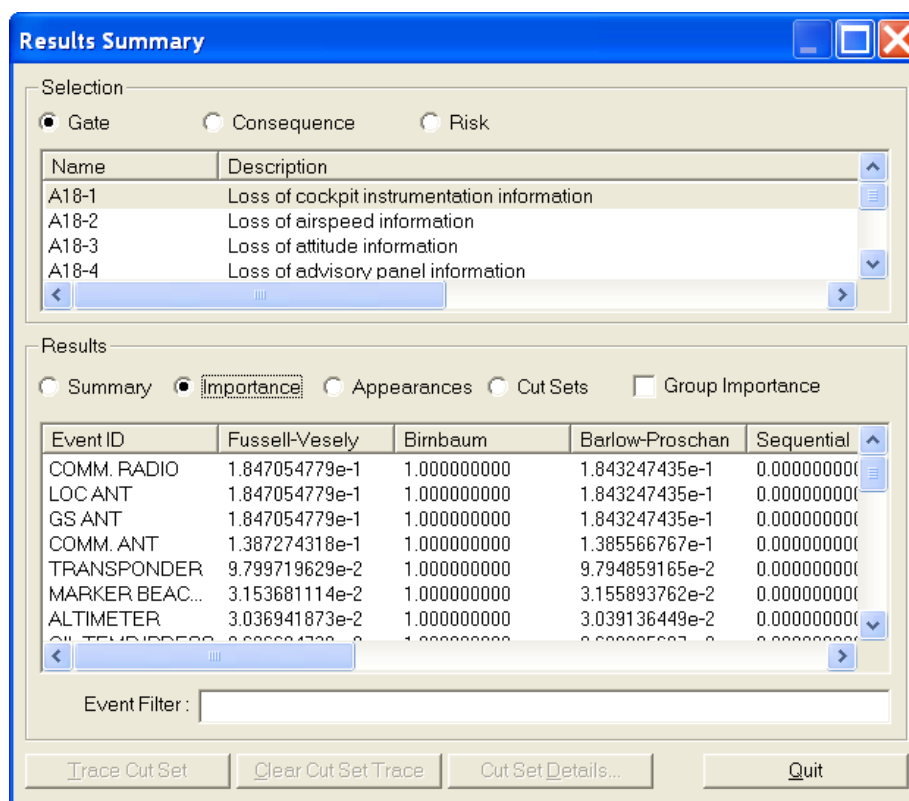


Figure 4 – Results Summary showing importance rankings

Reporting

One of the most important aspects of your reliability or safety studies is the creation of professional standard reports that will enable you to present the results in a clear and understandable form to colleagues, management, customers and regulatory bodies. The Isograph reliability software products share a common facility to produce reports containing text, graphs or diagrams. Your input data and output results from reliability applications are stored in a database. This information can be examined, filtered, sorted and displayed by the Report Generator. The Report Generator allows you to use reports supplied by Isograph to

print or print preview the data. A set of report formats appropriate to the product is supplied with each product.

You can also design your own reports, either from an empty report page or by copying one of the supplied reports and using that as the starting point.

The Report Generator also provides facilities for exporting reports to a variety of formats.

About Isograph

Isograph was founded in 1986 and is now one of the world's leading companies in the development and provision of integrated Reliability, Availability, Maintainability and Safety software products. The company has offices near Manchester in the UK and in Irvine, California. Isograph has over twenty distributors around the world providing local sales and support.

The Isograph software products are well proven and are used in many high profile projects. There are over 9000 installations worldwide. All of the Isograph software products are fully maintained and supported by a group of industry specialists. Training in the use of the software products is available at regular public courses or private on-site courses. Enhancements to the software products are largely driven by our user group community and associations with consultants and universities in the safety and reliability field.

Appendix A – Full System Description

A GA aircraft cockpit system is designed to provide the pilot with the information needed to safely fly the aircraft. Some information is critical to the flight, while some is not under normal flight conditions. The following instrumentation is the minimum required by Federal Aviation Regulations (FAR) Part 91 for a GA aircraft flying under Instrumentation Flight Rules (IFR) conditions:

- Airspeed indicator
- Altimeter
- Magnetic direction indicator
- Tachometer for each engine
- Oil pressure gauge for each engine
- Temperature gauge for each air-cooled engine
- Oil temperature gauge for each air-cooled engine
- Manifold pressure gauge for each engine if a variable pitch propeller is used
- Fuel gauge indicating the quality of the fuel in each tank
- Two-way radio communications and navigational equipment appropriate to the ground facilities to be used
- Gyroscopic rate of turn indicator
- Slip-skid indicator
- Altimeter adjustable for barometric pressure
- Clock displaying hours, minutes and seconds
- Generator or alternator
- Gyroscopic pitch and bank indicator (artificial horizon)
- Gyroscopic direction indicator (directional gyro or equivalent)

Cockpit reliability was defined as the probability that these instruments would provide the information for which they were designed. It was assumed that an instrument failed when it was not functioning normally or did not provide the accurate information, and that the cockpit failed if the required information was not provided by an instrument or combination of instruments.

Airspeed may be provided by one of three means. The airspeed indicator is the primary method of obtaining this information. This instrument calculates the airspeed by measuring the difference between the total air pressure and the atmospheric air pressure. Pressure readings may be affected by the build-up of ice on the pilot tube, so the tube contains a heating element powered by the alternator. The tachometer quantifies the engine power output. The airspeed may be deduced from this reading. The pilot may also contact the Air Traffic Control (ATC) centre. The ATC centre calculates and provides the pilot with the aircraft's ground speed.

Altitude information is normally provided by the altimeter. The altimeter measures the difference between the air pressure at the current altitude and that at a reference altitude (usually sea-level). Altitude may also be calculated from the aircraft's vertical speed and the

clock reading. This method is less accurate and assumed that the pilot knew the altitude at which the altimeter failed (FAA does not make allowances for the use of a watch in place of the advisory panel clock).

Attitude information consists of pitch, roll and yaw. The aircraft may go into an undesirable attitude if the pilot has no ground reference. This is a common problem at night in low visibility conditions. The attitude indication system (gyroscopic pitch, bank and direction indicators) and turning coordinator are the primary instruments for measuring attitude, requiring electrical and pneumatic power respectively. An increase in aircraft speed with no increase in engine power may also indicate that the aircraft is in a dive (pitch down). As the name suggests, the turn coordinator is used to make balanced turns. It reduces ‘skid’ and ‘side slip’, and increases turn efficiency. Yaw may be determined from the balance ball in the turn coordinator or directional gyro.

The **advisory panel** provides information about the status of the aircraft. This includes fuel quantity, oil temperature and pressure, pneumatic vacuum pressure and ammeter. The advisory panel instruments are not necessarily located in the same panel, so for the purposes of this report the advisory panel refers to the instruments and not to the panel itself.

Radio communications are required for entering certain airspaces. They are also required by the FAA for IFR flight. The transponder is considered to be part of the communications group, and is required to identify the aircraft to ATC.

Navigation is composed of three elements – vector navigation, radio navigation and pilotage. Vector navigation is used to transverse from one point to another using basic mathematics. Radio navigation is used to determine the aircraft’s position with respect to FAA navigational aids. The auto direction finder (ADF) and VHF omni range (VOR) are used for radio navigation. These instruments determine a bearing from a ground-based transmitter at a known position.

Airspeed and attitude information are needed to maintain lift and control of the aircraft. Altitude is very important to safe flying, especially in low-visibility conditions. The advisory panel alerts the pilot to the condition of the aircraft with information on engine status and fuel available. The communications system alerts the pilot to flying conditions and other aircraft. Navigation gets the aircraft to its destination, avoiding obstacles on the way. All information is gained from individual or groups of instruments, and there is considerable interdependence between groups.

This analysis includes some components and subsystems that are located outside the cockpit, but are still important as they supply data or power. These include the pilot tube system and the electrical power supply. All instruments aboard a GA aircraft are powered electrically with the exception of the directional gyro and attitude indicator, which are powered by vacuum pumps.

Only one source of electrical power is considered – the alternator. Failure of the alternator would cause the flight to be terminated as soon as possible, even though all of the instruments may be able to function for a limited time on battery power. Most cockpit instruments require electrical power.

Appendix B – The Full Fault Tree

