CHAPTER 29

FAULT / SUCCESS TREE ANALYSIS

CONTENTS

1 INTRODUCTION

1.1 This chapter explains the principles of fault and success tree construction and their use as a qualitative and quantitative prediction tool. Comments made in this chapter relate to both FTA and STA although they often only identify FTA. This is done to simplify the text and the comments can be read across.

1.2 A fault, or success, tree shows graphically, by means of a specified notation, the logical relationship between a particular system state or event and the basic failure/success causes. For a Fault Tree, normally, a ‘consequence’ will be a failure mode of the item or system being analysed. Alternatively, it may be a significant, undesirable, state[*] or event at the system level. Success Trees, on the other hand , address desirable states and events. The technique can be used:

a) qualitatively to illustrate the build up of states and event, identifying common elements in different branches (dependent failures) and defence in depth; and

b) quantitatively to give either the absolute probability of existence (for a state) or rate of occurrence (for an event) of the ‘consequence’, or the relative probabilities of various possible causes given that the ‘consequence’ has occurred.

1.3 The technique can be applied between any levels, e.g. system down to assembly level, Line Replaceable Unit (LRU) down to component level, etc. However, the TOP event and the level to which the analysis is to be taken must always be clearly specified.

1.4 The use of fault tree analysis benefits the design by:

a) directing the analyst to discover failures deductively;

b) indicating those parts of a system which are important with respect to the failure of interest;

c) providing a clear and concise means of imparting reliability information to management;

d) providing a means for qualitative or quantitative reliability analysis;

e) allowing the analyst to concentrate on one system failure mode, or ‘effect’, at a time;

[*] Note that it is essential in a fault or success tree to clearly identify which items are events (an instantaneous item characterized by a frequency of occurrence or probability of happening in a given time) and which are states (a condition that exists for a period of time and is characterized by a probability of existing at a given instant). The two are often referred to as ‘events’ in older treatises on analysis. Clarity is improved with the terminology ‘initiator events’ and ‘enabler events’. The terms ‘events’ and ‘states’ are recommended for future use.

However the terms ‘top event’ and ‘prime event’ or ‘basic event’ are ingrained into the terminology and can refer to states or events according to the context.

f) providing the analyst and designer with a clear understanding of the reliability characteristics and feature of the design;

g) enabling the analyst to identify possible reliability problems in a design even before detailed drawings have been competed; and

h) enabling human and other non-hardware failure causes to be evaluated.

1.5 Fault tree analysis does have practical limitation, mainly due to the time and effort involved, particularly in first time application. It requires very strict methodology and documentation if errors are to be avoided and care must be taken to select the most appropriate TOP events and levels of analysis so as to make the best use of available effort. Fault trees (or sub-trees of more general items, or parts of a system) which may be used again in other designs should be indexed and stored for future use.

2 DEFINITIONS

2.1 The technique of fault and success trees create a logical model of a scenario, expressed in states and events leading upto a given state or event. It is appropriate to define the terms used.

2.2 The top event is the starting point of developing the tree. It is the defined state or event that is to be analysed. Traditionally this has been drawn at the top of the page with the tree feeding up into it but this is not mandatory. The British Standard[5] places the top event at the right hand side of the page with the flow from left to right.

2.3 Prime events or basic events are the termination points of the analysis. These states or events are at the boundary of the model. For a quantified model it is essential to be able to assign a value (probability or frequency) to these items.

2.4 Gates are the logical functions which combine the states and events to form ‘super-states’ and ‘super-events’. Only simple gates should be used and the logical aspects of these are described in PtDCh1. Where the experienced analyst uses more complicated gate types, then a full explanation of the logical and arithmetical process should be given in the report on the analysis.

2.5 A state is a condition that exists for a period of time and is characterized by a probability of existing at a given instant. For example a door being closed is a state. States are sometimes referred to as enabler events.

2.6 An event is an instantaneous occurrence characterized by a frequency of occurrence or probability of happening in a given time. For example a man walking through a doorway. If the door is closed (state) then he will band his nose (super-event). Events are sometimes referred to as initiator events.

3 FEATURES AND ANALYSIS

3.1 In a Fault Tree the TOP event of the tree is a system failed state or a system failure event and the PRIME events of the tree are element states and events that cause the system failure (and are usually element failures). Examples of system failed states include ‘forward radar failed', 'flat battery' and 'Ship aground'. Examples of system failure events include 'collision with another ship', 'man falls down ladder' and 'uncommanded missile launch'.

3.2 In a Success Tree the TOP event is system success (state or event) and the PRIME events are states or events that lead to success (usually element success states). Examples of success include 'mission completed' (event), 'fire extinguished' (event) and 'radar operating' (state).

3.3 The example in Leaflet 1 discusses a system that is represented by a Fault Tree. A Success Tree could equally have been used, by replacing all PRIME event states by their inverse state (elements down by elements up) and by replacing AND gates by OR gates and vice versa. Indeed it is possible to convert between success and fault trees in one tree by using not gates but this is not recommended.

3.4 Fault Tree Analysis (FTA) and Success Tree Analysis (STA) provide an objective basis for analysing system design, performing trade-off studies, analysing 'Dependant Failures', assessing compliance with safety requirements and justifying design improvements or additions. The 'top down' approach makes the technique particularly suitable for starting reliability design evaluation during the early stages of a project (e.g. project definition) and analysing potential accidents and hazards. It can be used qualitatively to identity those items within a design that are likely to contribute most to a particular system failure and therefore merit closest attention. In this respect, FTA can be considered as a complementary technique to Failure Mode and Effect Analysis (FMEA); that is, FTA can identify potentially critical items during the early design stage for deeper analysis during the detailed design stage using FMEA. A further feature of FTA is that being event orientated, it can include failure causes such as 'operator error' and can therefore be used to evaluate safety requirements or maintenance requirements, etc.

3.5 FTA/STA involves the following main steps:

a) definition of the system, eg the items comprising the system, their functional relationship and performance requirements.

b) definition of the TOP event to be analysed and the bounds of the analysis;

c) construction of the fault tree by tracing the TOP event (failure) down to one or more causes at the specified functional (or item) level within the design;

d) calculation of the probability or frequency of the TOP event; and

e) reporting on the analysis carried out.

3.6 The following sections address the construction and calcualation aspects of the process. System definition (apart from comments made under construction) and reporting are as for other techniques.

4 CONSTRUCTION

4.1 General

4.1.1 The principles of fault tree construction and its use for prediction are amplified and illustrated by an example in Leaflet 6/1.

4.1.2 The term 'tree' is used because the diagrammatic representation of the analysis has a branching structure which increases in size as various levels of details are considered. In fact the structure is more analogous to the roots of a tree, since the normal convention for constructing a fault tree is to start at the top of the page with the 'consequence' or system failure mode being considered, then represent underneath the causes which could lead to the 'consequence', in increasing details as one progresses down the page. For this reason the 'consequence', or failure mode under consideration, is called the TOP event. The lowest levels of cause to which the tree goes comprise the PRIME eventsFigure 1 indicates that the branches (or roots) of a fault tree generally combine in the form of Boolean logic statements (see PtDCh1). That is, they are either AND or OR statements.

4.1.3 Starting at the to of the page and working down is not mandatory. The British Standard[5] places the TOP event on the right hand side of the page and works to the left. The flow of the scenario model is then from left to right instead of bottom to top. The analyst is free to choose the orientation to best present the results to the reader.

4.2 Notation

4.2.1 A basic feature of the notation is the representation of states, events (including different types of state and event) and logical gates. In older trees the gates were drawn large enough to write the text describing the sate or event in the symbol. More modern practice is to use a rectangular box for the text with a smaller gate or termination symbol underneath. Other differences exist between the exact symbology used. The is recommended to use a reasonably standard form (see Figure 1) and explain any unusual features in the report.

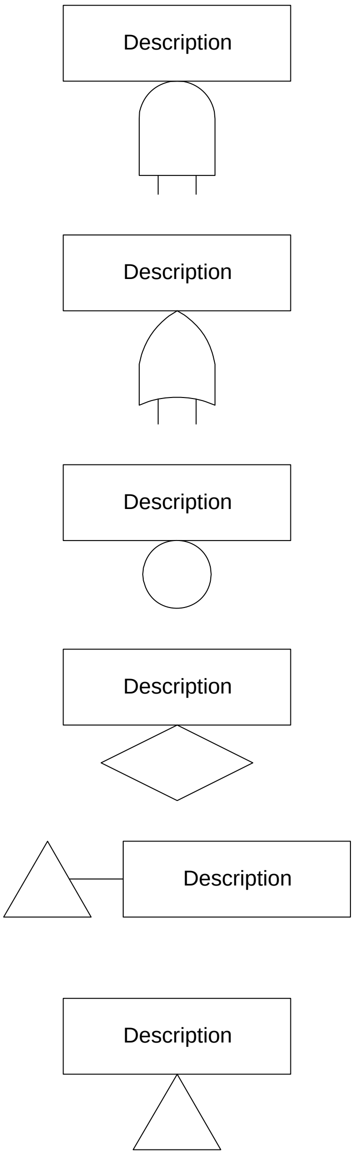
4.2.2 Additional logic and event symbols may be required, for example, to represent majority voting events, or to indicate a required sequence of events by employing an Initiator/Enabler gate. Different fault tree packages use different symbols for less common gates; the use of these symbols should be formally documented.

4.2.3 The IEC Standard 1025 and British Standard 5760 (Part 7)[5] specify alternative symbols which may be used to indicate the gate type. These symbols are displayed in a square and include '&' for and AND gate and '>=1' for an OR gate. When using these symbols, the British Standard[5] should be referred to.

4.2.4 Careful attention should be paid to the description of the states and events that is entered. The description needs to clearly identify what, specifically, is happening without being too dependent on the context or too specific as to exclude relevant situations. For example a state of 'light bulb failed' when analysing a car lighting system is too general if the tree has already separated front, back and interior lights. A software package should regard the same description in different areas of the tree as a dependent failure. Different failures should have different descriptions.

4.2.5 The description should also distinguish between states and events in the text. The use of a box with rounded corners to indicate states and square corners for events has been used but this is rare. More common is the technique of using different initial letters in an item enumeration label.

4.2.6 A complete tree will terminate in circles and diamonds representing states and events for which reliability information is necessary to the fault tree. Events that appear as circles or diamonds are treated as Prime Events.



State or event with AND gate. The state or event will exist or occur when all of the inputs exist or occur.

State or event with OR Gate. The state or event will exist or occur when any one or more of the inputs exist or occur.

Basic or prime state or event. This item is statistically independent of all other states and events and can be ascribed a probability or frequency from other analysis.

A basic state or event that has not been fully developed. This may be due to insignificance or the lack of information.

A transfer out state or event. This item feeds to a transfer in item on another sheet of the analysis. A label (often an alphanumeric character) is normally placed in the triangle and will match the label of a transfer in.

A transfer in state or event. This item is fed from a transfer out state or event on a different sheet.

Figure 1: Typical Fault Tree Logic and Event Symbols

5 ANALYSIS

5.1 The first point of interest is which prime events, or combinations of prime events, are necessary to cause the failure under consideration. These are termed ‘Minimal Cut Sets’.

5.2 The minimal cut sets may often be determined by inspection of the fault tree. However more formal and sophisticated procedures are usually necessary as the tree increases in size and complexity.

5.3 Cut sets are referred to as ‘first order’, ‘second order’ etc. First order cut sets are items that cause the top event directly. Second order cut sets require two states to exist concurrently or states to exist when an event occurs. Higher order cut sets follow the same pattern. The lowest order of cut set is linked to the design philosophy of defence in depth. It may be a design target to have no first order cut sets. FTA provides a technique for the verification of such requirements.

5.4 Having determined the minimal cut sets, they can be evaluated qualitatively or quantitatively to assess their relative significance. In the example in Leaflet 1, assuming that ‘Multiple Failure of Liquid Crystals’ (1) is a most unlikely event, prime events 2 and 3 would appear to be the areas of greatest risk. A qualitative assessment of their potential risk would require, for example, the switch design to be examined to determine the likelihood of the switch failing at ‘off’ and the type and extent of internal wiring and joints to be checked to see whether any improvements might be made to reduce the likelihood of failure. Quantitative assessments of minimal cut sets may involve some form of simulation using failure data for each of the prime events and normally this is best done by computer. Note that if a particular prime event appears in more than one minimal cut set, it will merit close attention because there is more than one path by which it contributes to the TOP event.

5.5 The construction and analysis of fault trees are separate tasks but there will usually be some interaction between the two. For example, during the analysis the designer may come aware of features that were overlooked during the construction of the fault tree. For this reason, qualitative evaluation can be very profitable because it develops considerable understanding of the design.

6 PROBABILITY CALCULATIONS

6.1 Quantitative analysis of a fault tree provides the means to determine in absolute terms which events are most critical to the achievement of the TOP event and, therefore, where improvements would be most beneficial. It also provides the means to predict the frequency or probability of the TOP event occurring (or not) given the probabilities of occurrence of the PRIME events.

6.2 There are two main methods of performing the quantitative analysis: working up the tree and via the cut sets. Each has advantages and disadvantages and a choice should be made for the individual analysis.

6.3 The first method requires each gate to be calculated in turn. For example (in Leaflet 1) the instantaneous probability of ‘low or no power from charger’ (item O3) is the sum of the instantaneous probabilities of items 4 (faulty transformer), 5, 6 and 7. There is a proviso that the items must be independent. This process is repeated for each gate until the TOP event is reached.

6.4 The second method identifies all the cut sets that lead to the TOP events, evaluates each one and sums the results. This method has the advantage of dealing with the dependent failures but care is still needed that independence is achieved prior the summation.

6.5 For AND and OR gates the probabilities are easily calculated:

$$P_{(\text{AND gate})} = \prod P_{(\text{input i})}$$

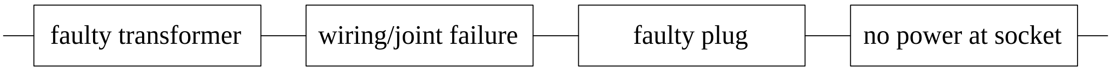
$$P_{(\text{OR gate})} = 1 - \prod (1 - P_{(\text{input i})})$$

$$\text{or } P_{(\text{OR gate})} = \sum P_{(\text{input i})} \text{ when } P_{(\text{input i})} \ll 1$$

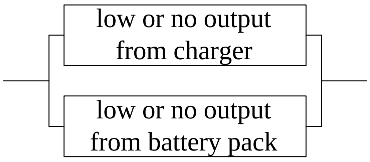
6.6 The example in Leaflet 1 addresses the probability of the failed state existing. This is the inverse of the availability of the display (the unavailability). All the 'events' identified are states and it is the unavailability that calculated.

6.7 Event rates can also be entered into the calculations where appropriate. However the rules of mathematics must be observed.

6.8 Reliability calculations can be undertaken using a fault tree in essentially the same manner as is described for Reliability Block Diagrams (RBD) in PtDCh6. This is possible because both types of diagram are to a great extent equivalent. That is, in their simplest forms, they are both representations of Boolean logic. For example, the event 'low or no output from the charger' (see Gate O3 on Leaflet 1) can be represented by:



The event 'power supply failure' (see Gate Al on Figure 3) can be represented by:


low or no output from charger
low or no output from battery pack

Thus:

a) an 'OR gate' represents SERIES reliability dependency.

b) an 'AND gate' represents REDUNDANCY.

6.9 Using the expressions contained in PtDCh6, the reliability that applies at each 'gate output' event can be computed progressively until the value is obtained for the TOP event. For example, the reliability (R_S) of a 'series' system of N elements is given by:

$$R_S = R_1 \text{ x } R_2 \text{ x } R_3 \ldots\ldots \text{x } R_n$$

6.10 Thus, referring to Leaflet 1, the probability of surviving 'low or no output from charger' (i.e. the event not occurring) would be the product of the 'survival' probabilities of events 4, 5, 6 and 7.

7 BRIEF GUIDELINES

7.1 FTA and STA provide useful methods for analysing the scenario leading to identified states and events. The state or event being analysed is normally referred to as the TOP event.

7.2 This Chapter provides only a simple introduction to fault tree analysis, using an example chosen to be familiar to most readers. Generally, a more sophisticated approach will be required than is illustrated here; for example, statistical independence will not hold if standby redundancy is involved. PtDCh6 and PtDCh1 provide guidance on the methods suitable for quantitative analysis.

7.3 The competent engineer can use the method as a basis and develop the model (in a mathematically sound manner) to illustrate a large variety of scenarios. It is not the place of this chapter to extend the theory in this area as it requires some experience with the technique. Any such extension must be fully explained in the analysis report that the tree contributes to.

7.4 It is important that dependant failures are included in the fault tree diagram as they can negate the effects of designed redundancy on the reliability performance of a system. In many cases, dependant failures can affect the unavailability of a system by several orders of magnitude.

7.5 Care is required that only states or only events combine in an OR gate and that only one event feeds into an AND gate (the other inputs must be states). The inputs to an AND gate can all be states.

7.6 In certain circumstances the order in which events take place must be taken into consideration when evaluating the frequency of a fault tree TOP event., i.e. Initiator/Enabler Events. This is a complex subject and the analyst needs to identify the situation clearly and express it in the wording of the state and event descriptions.

7.7 The descriptive information included in the event symbol boxes should be precise enough to be specific, but at the same time sufficiently general to avoid missing items, i.e. state precisely what the item is, when it occurs and whether it is state or an event.

7.8 Ensure that the assumptions made by some computer based analysis tools are fully understood before constructing or analysing a tree. Some packages make low number approximations.

Intentional blank page

LEAFLET 29/0

RELATED DOCUMENTS

1. DEF STAN 00-40 (Part 1)/Issue 2 (R&MP-1). 14 December 1994. *Reliability and Maintainability Part 1: Management Responsibilities and Requirements for Programmes and Plans.*

2. DEF STAN 00-40 (Part 2)/Issue 1 (R&MP-2). 14 December 1994. *Reliability and Maintainability Part 2: General Application Guidance on the Use of Part 1 (R&MP-1).*

3. DEF STAN 00-41 Issue 3. 25 June 1993. *Reliability and Maintainability MOD Guide to Practices and Procedures.*

4. NUREG-0492. *Fault Tree Handbook.* US Nuclear Regulator Commission. January 1981.

5. BS 5760: Part 7: 1991. *Reliability of System, Equipment and Components.*

6. J D Andrews & T R Moss. *Reliability and Risk Assessment.* Longman Scientific and Technical. 1993.

7. E J Henley & H Kumamoto. *Reliability Engineering and Risk Assessment*. Prentice-Hall. 1981.

8. A E Green & A J Bourne. *Reliability Technology*. Wiley. 1972.

Intentional blank page

LEAFLET 29/1

FAULT TREE EXAMPLE

8 INTRODUCTION

8.1 To provide a simple introduction to fault tree analysis, an example has been chosen which will be familiar to most readers, whatever their specialisation. Assume that the analysis is concerned with a pocket calculator with rechargeable batteries and the particular 'consequence' (i.e. failure mode or TOP event) under consideration is 'No Liquid Crystal Display'. Causes could be assigned to the TOP event and, in turn, further causes could be assigned to those causes, as shown in Figure 1.

8.2 Further examination is then made of a mission whereby the Calculator and Charger discussed are to be taken to a meeting at which they will be operated for 3 hours. What is the probability that the calculator and charger survive this 'mission' without the failure mode 'No Liquid Crystal Display' occurring?

9 PUT BOUNDS ON THE PROBLEM

9.1 It is clear from Figure 1 that the technique has great flexibility since the analysis could be stopped at any level of 'cause'. On the other hand, it could be carried on indefinitely, even to considering all possible failure modes of the national grid that could prevent power at the socket into which the charger is plugged! In fault tree analysis, there is always some aspect that must be considered external to the problem and hence constitutes a bound. In most cases, the analysis will be concerned with failures within a system and this will normally define the external bounds. However, the depth to which causes are assigned within the system is also a bound and so the level of the 'prime events' must be defined.

9.2 In this case it is taken the boundary is taken to be the power supply socket and the user keys, switch and display. Ergonomic issues and other human factors issues are deemed outside the scope.

10 TREE CONSTRUCTION

10.1 Figure 1 is termed 'Preliminary Fault Tree' because it is not necessarily comprehensive and is not, in fact, how the tree would be drawn in practice. It provides an outline of the tree, as it will eventually be and identifies the key areas.

10.2 The gates can then be added starting at the top and completing each set of contributing events before moving on to the next gate. The descriptions need to be completed at this stage and the logical integrity of the comments made confirmed.

10.3 It is notable that all the ‘events; in this tree are states. They all exist from failure to repair. As such the tree address the availability and produces the probability that the calculator will work when required.

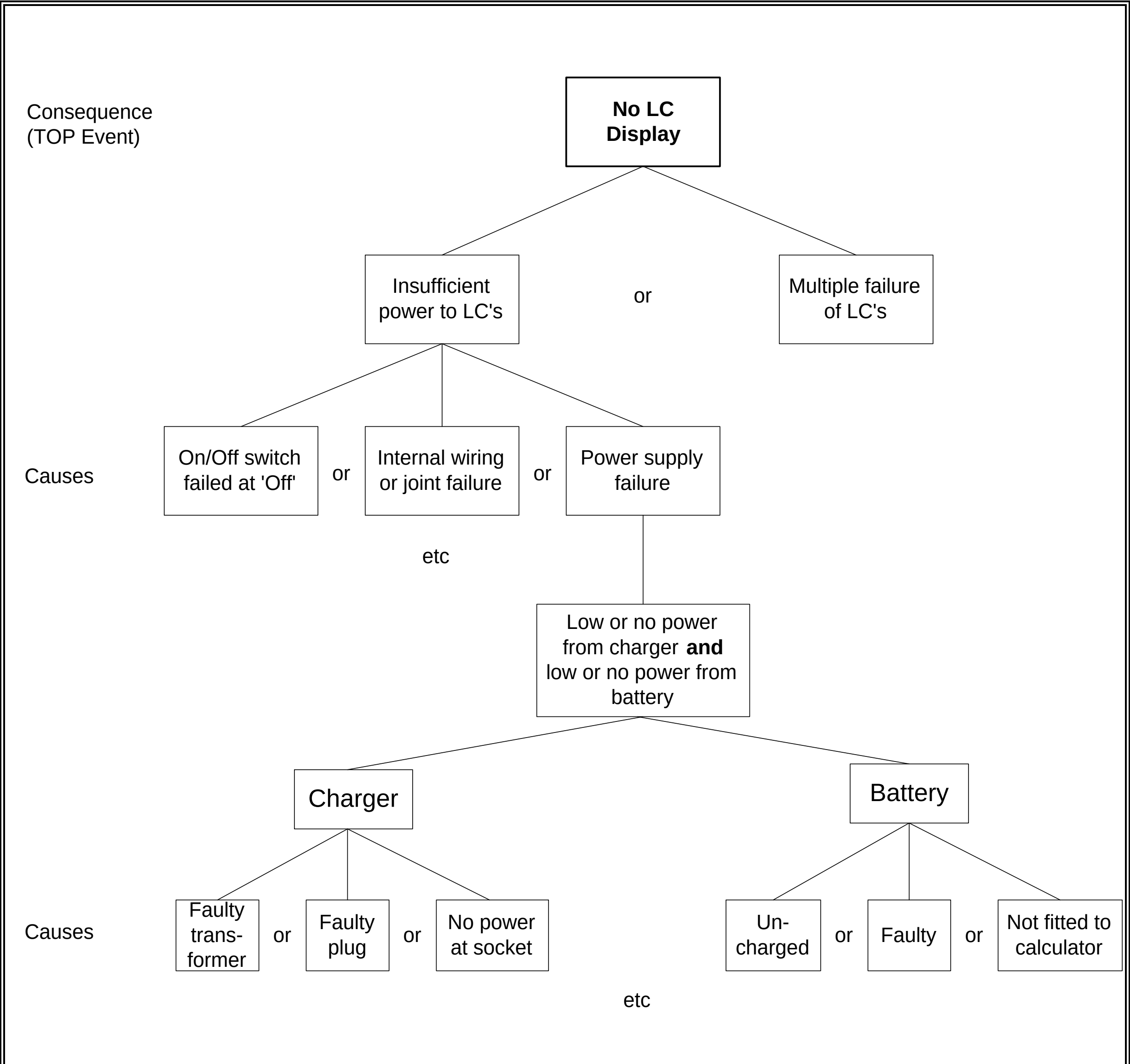
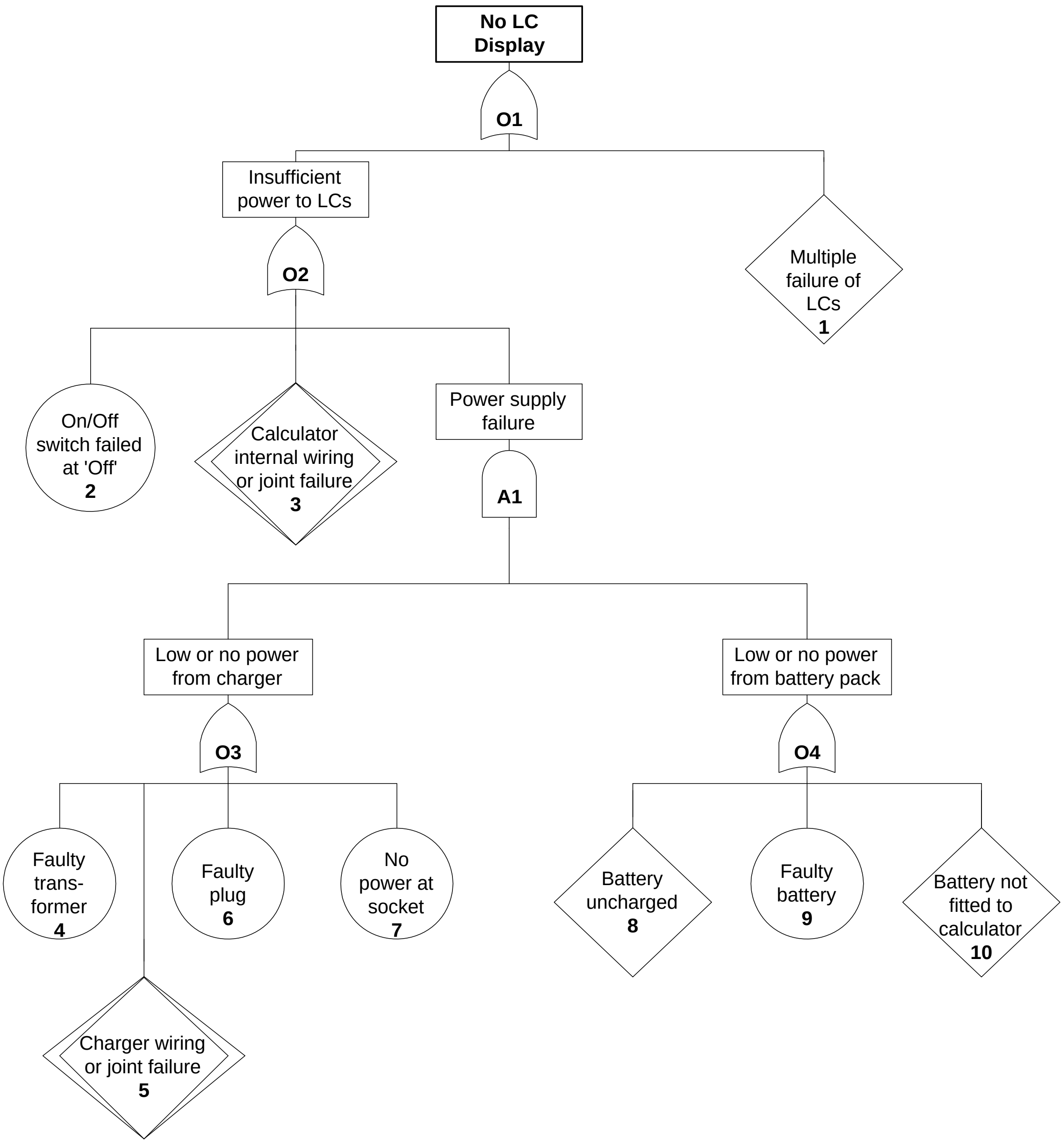


Figure 2: Preliminary Fault Tree

10.4 It should also be noted that the inputs to an OR gate must be all states or all events. Likewise the inputs to an AND gate must be all states or one event and all the others inputs states. This is a mathematical requirement as a non-dimensional probability can not be added to a frequency nor has the product of two frequencies any meaning. The appearance of such situations in a tree is an error and needs to be resolved. This may require careful consideration (was the paint pot in mid-air when the man walked under the ladder or the man under the ladder when the paint pot fell?) and the situation modelled in the most appropriate manner.

10.5 Even from this simple example, it can be seen that the construction of a fault tree requires a detailed understanding of the design and therefore involves a close co-operation with the designer. It also illustrates that fault trees of more complex systems are likely to occupy large numbers of pages, each of which must be clearly identified, defined and indexed if errors are to be avoided.


No LC Display
O1
Insufficient power to LCs
Multiple failure of LCs
1
O2
On/Off switch failed at 'Off'
2
Calculator internal wiring or joint failure
3
Power supply failure
A1
Low or no power from charger
Low or no power from battery pack
O3
O4
Faulty trans-former
4
Faulty plug
6
No power at socket
7
Battery uncharged
8
Faulty battery
9
Battery not fitted to calculator
10
Charger wiring or joint failure
5

Notes:

1. It is useful to label gates.
   In this Figure OR gates are labelled O1, O2, O3, etc.; AND gates A1, A2, etc.
2. For ease of reference in the text, prime events are labelled 1 to 10.

Figure 3: Fault Tree using Logic and Event Symbols

11 ANALYSIS

11.1 The cut sets (by inspection) are:

1

2

3

4 . 8

4 . 9

4 . 10

5 . 8

and all other combinations of 4+5+6+7 and 8+9+10

11.2 There are three first order cut sets. However, item 1, multiple failure of LCs, is likely to have a low probability leaving the switch and the wiring. The second cut sets are also reasonably likely and need to be considered in the design.

12 CALCULATIONS

12.1 Step 1. Probabilities of ‘survival’ (or not surviving) must be determined for each prime event. Since the problem is concerned with the calculator system itself, event 7 (No power at mains) is beyond the bounds of the problem and can be ignored (set the probability to 0). Assume that the assessments made for the other prime events on the basis of failure rate lists, past experience, etc, are as given below. (Note that these are invented for this example only and should not in any way be considered realistic).

Prime Event	No.	Probability of Survival
Multiple failure of LCs	(1)	0.99999 (the probability of all liquid crystals failing must by very small, ignoring mis-use or handling damage beyond the ‘spec’)
On/Off switch failed at ‘Off’	(2)	0.995
Calculator internal wiring or joint failure	(3)	0.999
Faulty transformer	(4)	0.995
Charger wiring or joint failure	(5)	0.999
Faulty plug	(6)	0.99
No power at socket	(7)	Beyond bounds of problem therefore ignored, i.e. assigned Probability of Survival = 1.0

Battery uncharged	(8)	0.9
Faulty battery	(9)	0.99
Battery not fitted to calculator	(10)	0.95

Note that event 10 (No battery) could well be considered beyond the bounds of the problem since it is a failure of ‘maintenance’ or user mis-management. It will be included, however, in this example.

12.2 Step 2. These probabilities are now combined progressively to provide an assessment for the TOP event.

(i) Gate O3. An ‘OR gate’ represents series reliability dependency. Hence:

Probability of NOT experiencing low or no output from charger

= 0.995 x 0.999 x 0.99 x 1.0

= 0.984065

(or failure probability = 0.015935)

(ii) Gate O4. An ‘OR gate’ and hence:

Probability of NOT experiencing low or no power from battery pack

= 0.9 x 0.99 x 0.95

= 0.846450

(or failure probability = 0.153550).

(iii) Gate A1. An ‘AND gate’ represents redundancy and hence, calculation is simplified by first considering probabilities of failure:

Probability of power supply failure

Gate O3 x Gate O4 failure probabilities

= 0.015935 x 0.153550

= 0.002447

Probability of NO power supply failure

= 1 - 0.002447

= 0.997553

(iv) Gate O2. An 'OR gate' and hence:

Probability of NOT having insufficient or no power to LCs

= Event 2 x Event 3 x Gate A1 survival probabilities

= 0.995 x 0.999 x 0.997553

= 0.991573

(v) Gate O1. An 'OR gate' and hence:

Probability that the Liquid Crystal Display survives for the 'mission'

= Event 1 x Gate O2 survival probabilities

= 0.99999 x 0.991573

= 0.991563

$\underline{\cong 0.992}$

This is the answer to the problem set. It should however be rounded as the input data is not accurate to 4 significant figures. In rounding probabilities of the nature, it is the difference from unity that should be rounded, not the absolute number.

12.3 Looked at another way, the probability of this 'TOP event' failure mode occurring during the 'mission' (the 3 hour meeting) is:

1 - 0.992 = $\underline{0.008}$