IEC 61025

Edition 2.0 2006-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Fault tree analysis (FTA)

Analyse par arbre de panne (AAP)

IEC 61025:2006

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61025

Edition 2.0 2006-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Fault tree analysis (FTA)

Analyse par arbre de panne (AAP)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XA
CODE PRIX

ICS 03.120.01; 03.120.99

ISBN 2-8318-8918-9

CONTENTS

FOREWORD 4
INTRODUCTION 6

1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 Symbols 10
5 General 11
5.1 Fault tree description and structure 11
5.2 Objectives 12
5.3 Applications 12
5.4 Combinations with other reliability analysis techniques 13
6 Development and evaluation 15
6.1 General considerations 15
6.2 Required system information 18
6.3 Fault tree graphical description and structure 19
7 Fault tree development and evaluation 20
7.1 General 20
7.2 Scope of analysis 20
7.3 System familiarization 20
7.4 Fault tree development 20
7.5 Fault tree construction 21
7.6 Failure rates in fault tree analysis 38
8 Identification and labelling in a fault tree 38
9 Report 39

Annex A (informative) Symbols 41
Annex B (informative) Detailed procedure for disjointing 48

Bibliography 52

Figure 1 – Explanation of terms used in fault tree analyses 10
Figure 2 – Fault tree representation of a series structure 23
Figure 3 – Fault tree representation of parallel, active redundancy 24
Figure 4 – En example of fault tree showing different gate types 26
Figure 5 – Rectangular gate and events representation 27
Figure 6 – An example fault tree containing a repeated and a transfer event 28
Figure 7 – Example showing common cause considerations in rectangular gate representation 28
Figure 8 – Bridge circuit example to be analysed by a fault tree 32
Figure 9 – Fault tree representation of the bridge circuit 33
Figure 10 – Bridge system FTA, Esary-Proschan, no disjointing 35

Figure 11 – Bridge system probability of failure calculated with rare-event approximation 36
Figure 12 – Probability of occurrence of the top event with disjointing 37
Figure A.1 – Example of a PAND gate 47

Table A.1 – Frequently used symbols for a fault tree 41
Table A.2 – Common symbols for events and event description 44
Table A.3 – Static gates 45
Table A.4 – Dynamic gates 46

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FAULT TREE ANALYSIS (FTA)

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61025 has been prepared by IEC technical committee 56: Dependability.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1142/FDIS	56/1162/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This second edition cancels and replaces the first edition, published in 1990, and constitutes a technical revision.

The main changes with respect to the previous edition are as follows:

– added detailed explanations of fault tree methodologies
– added quantitative and reliability aspects of Fault Tree Analysis (FTA)
– expanded relationship with other dependability techniques
– added examples of analyses and methods explained in this standard
– updated symbols currently in use

Clause 7, dealing with analysis, has been revised to address traditional logic fault tree analysis separately from the quantitative analysis that has been used for many years already, for reliability improvement of products in their development stage.

Some material included previously in the body of this standard has been transferred to Annexes A and B.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

Fault tree analysis (FTA) is concerned with the identification and analysis of conditions and factors that cause or may potentially cause or contribute to the occurrence of a defined top event. With FTA this event is usually seizure or degradation of system perfomance, safety or other important operational attributes, while with STA (success tree analysis) this event is the attribute describing the success.

FTA is often applied to the safety analysis of systems (such as transportation systems, power plants, or any other systems that might require evaluation of safety of their operation). Fault tree analysis can be also used for availability and maintainability analysis. However, for simplicity, in the rest of this standard the term “reliability” will be used to represent these aspects of system performance.

This standard addresses two approaches to FTA. One is a qualitative approach, where the probability of events and their contributing factors, – input events – or their frequency of occurrence is not addressed. This approach is a detailed analysis of events/faults and is known as a qualitative or traditional FTA. It is largely used in nuclear industry applications and many other instances where the potential causes or faults are sought out, without interest in their likelihood of occurrence. At times, some events in the traditional FTA are investigated quantitatively, but these calculations are disassociated with any overall reliability concepts, in which case, no attempt to calculate overall reliability using FTA is made. The second approach, adopted by many industries, is largely quantitative, where a detailed FTA models an entire product, process or system, and the vast majority of the basic events, whether faults or events, has a probability of occurrence determined by analysis or test. In this case, the final result is the probability of occurrence of a top event representing reliability or probability of fault or a failure.

FAULT TREE ANALYSIS (FTA)

1 Scope

This International Standard describes fault tree analysis and provides guidance on its application as follows:

– definition of basic principles;
  - describing and explaining the associated mathematical modelling;
  - explaining the relationships of FTA to other reliability modelling techniques;
– description of the steps involved in performing the FTA;
– identification of appropriate assumptions, events and failure modes;
– identification and description of commonly used symbols.

2 Normative references

The following referenced documents are indispensable for the application of this document. For the references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050(191), *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 61165, *Application of Markov techniques*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050(191) apply.

In fault tree methodology and applications, many terms are used to better explain the intent of analysis or the thought process behind such analysis. There are terms used also as synonyms to those that are considered analytically correct by various authors. The following additional terms are used in this standard.

3.1
outcome
result of an action or other input; a consequence of a cause

NOTE 1 An outcome can be an event or a state. Within a fault tree, an outcome from a combination of corresponding input events represented by a gate may be either an intermediate event or a top event.

NOTE 2 Within a fault tree, an outcome may also be an input to an intermediate event, or it can be the top event.

3.2
top event
outcome of combinations of all input events

NOTE 1 It is the event of interest under which a fault tree is developed. The top event is often referred to as the **final event,** or as **the top outcome**.

NOTE 2 It is pre-defined and is a starting point of a fault tree. It has the top position in the hierarchy of events.

3.3
final event
final result of combinations of all of the input, intermediate and basic events

NOTE It is a result of input events or states (see 3.2).

3.4
top outcome
outcome that is investigated by building the fault tree

NOTE Final result of combinations of all of the input, intermediate and basic events; it is a result of input events or states (see 3.2).

3.5
gate
symbol which is used to establish symbolic link between the output event and the corresponding inputs

NOTE A given gate symbol reflects the type of relationship required between the input events for the output event to occur.

3.6
cut set
group of events that, if all occur, would cause occurrence of the top event

3.7
minimal cut set
minimum, or the smallest set of events needed to occur to cause the top event

NOTE The non-occurrence of any one of the events in the set would prevent the occurrence of the top event.

3.8
event
occurrence of a condition or an action

3.9
basic event
event or state that cannot be further developed

3.10
primary event
event that is at the bottom of the fault tree

NOTE In this standard, primary event can mean a basic event that need not be developed any more, or it can be an event that, although a product of groups of events and gates, may be developed elsewhere, or may not be developed at all (undeveloped event).

3.11
intermediate event
event that is neither a top event nor a primary event

NOTE It is usually a result of one or more primary and/or other intermediate events.

3.12
undeveloped event
event that does not have any input events

NOTE It is not developed in the analysis for various possible reasons, such as lack of more detailed information, or it is developed in another analysis and then annotated in the current analysis as undeveloped. An example of undeveloped gates could be Commercial Off The Shelf Items (or COTS).

3.13
single point failure (event)
failure event which, if it occurs, would cause overall system failure or would, by itself regardless of other events or their combinations, cause the top unfavourable event (outcome)

3.14
common cause events
different events in a system or a fault tree that have the same cause for their occurrence

NOTE An example of such an event would be shorting of ceramic capacitors due to flexing of the printed circuit board; thus, even though these might be different capacitors having different functions in their design, their shorting would have the same cause – the same input event.

3.15
common cause
cause of occurrence of multiple events

NOTE In the above example it would be board flexing that itself can be an intermediate event resulting from multiple events such as environmental shock, vibrations or manual printing circuit board break during product manufacturing.

3.16
replicated or repeated event
event that is an input to more than one higher level event

NOTE This event can be a common cause or a failure mode of a component, shared by more than one part of a design.

Figure 1 illustrates some of the above definitions. This figure contains annotations and description of events to better explain the practical application of a fault tree. Omitted from Figure 1 are the graphical explanations of cut sets or minimal cut sets, for simplicity of the graphical representation of other pertinent terms. The symbols in Figure 1 and all of the subsequent figures appear somewhat different to those in Tables A.1, A.2, A.3, and A.4 because of the added box above the gate symbol for description of individual events.

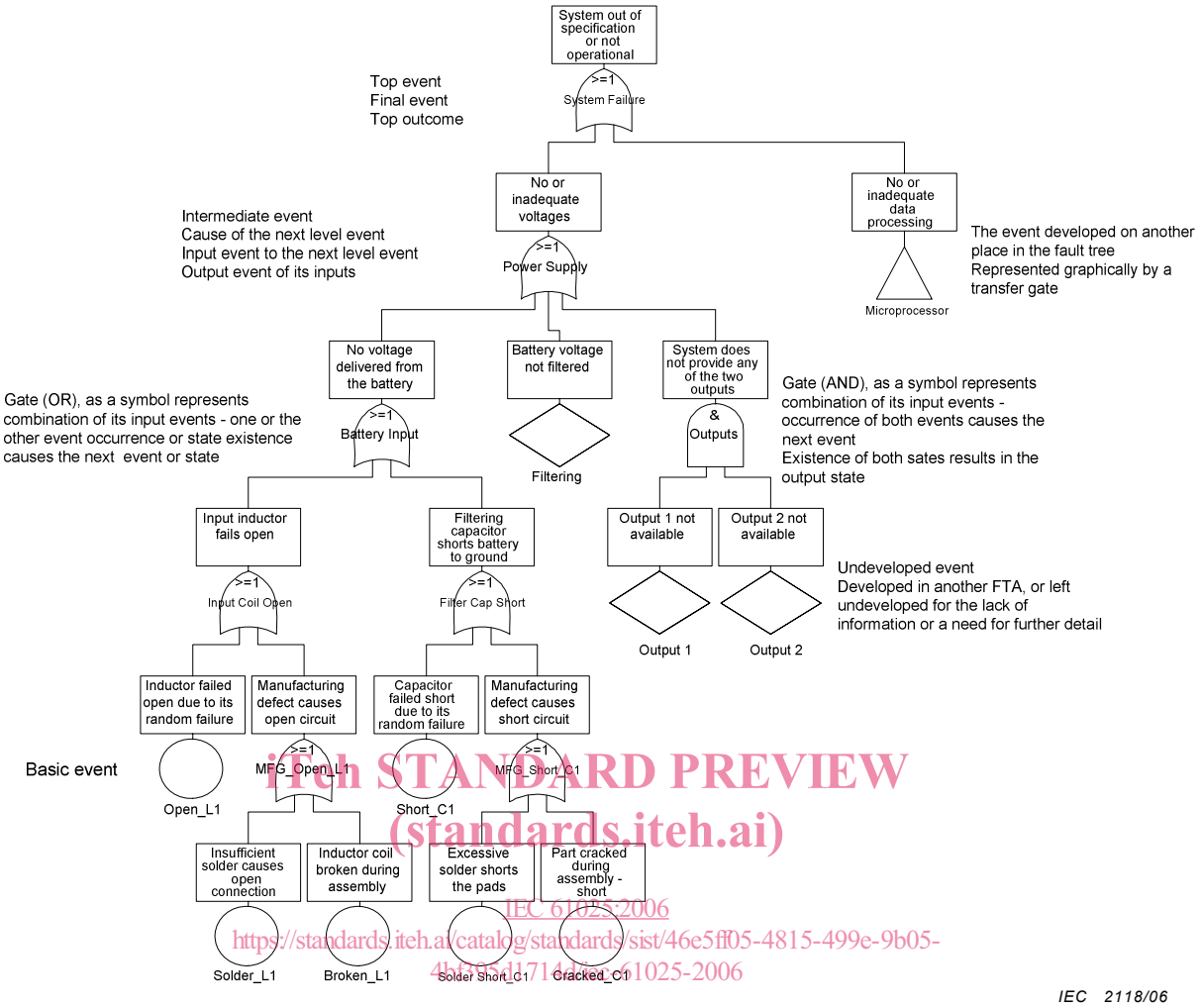

Figure 1 – Explanation of terms used in fault tree analyses

NOTE Symbols in Figure 1 and all other figures might slightly differ from the symbols shown in Annex A. This is because description blocks are added to better explain the relationship of various events

4 Symbols

The graphical representation of a fault tree requires that symbols, identifiers and labels be used in a consistent manner. Symbols describing fault tree events vary with user preferences and software packages, when used. General guidance is given in Clause 8 and in Annex A.

Other symbols used in this standard are standard dependability symbols such as $F(t)$ or just probability of an event occurring F. For that reason, a separate list of symbols is not provided.

5 General

5.1 Fault tree description and structure

Several analytical methods of dependability analysis are available, of which fault tree analysis (FTA) is one. The purpose of each method and their individual or combined applicability in evaluating the flow of events or states that would be the cause of an outcome, or reliability and availability of a given system or component should be examined by the analyst before starting FTA. Consideration should be given to the advantages and disadvantages of each method and their respective products, data required to perform the analysis, complexity of analysis and other factors identified in this standard.

A fault tree is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined outcome, referred to as the "top event". When the outcome is a success, then the fault tree becomes a success tree, where the input events are those that contribute to the top success event. The representation of a fault tree is in a form that can be clearly understood, analysed and, as necessary, rearranged to facilitate the identification of:

– factors affecting the investigated top event as it is carried out in most of the traditional fault tree analyses;

– factors affecting the reliability and performance characteristics of the system, when the FTA technique is used for reliability analysis, for example design deficiencies, environmental or operational stresses, component failure modes, operator mistakes, software faults;

– events affecting more than one functional component, which could cancel the benefits of specific redundancies or affect two or more parts of a product that may otherwise seem operationally unrelated or independent (common cause events).

Fault tree analysis is a deductive (top-down) method of analysis aimed at pinpointing the causes or combinations of causes that can lead to the defined top event. The analysis can be qualitative or quantitative, depending on the scope of the analyses.

A fault tree can be developed as its complement, the success tree analysis, (STA), where the top event is a success, and its inputs are contributor to the success (desired) event.

In cases where the probability of occurrence of the primary events cannot be estimated, a qualitative FTA may be used to investigate causes of potential unfavourable outcomes with individual primary events marked with descriptive likelihood of occurrence such as: “highly probable”, “very probable” “medium probability”, “remote probability”, etc. The primary goal of the qualitative FTA is to identify the minimal cut set in order to determine the ways in which the basic or primary events influence the top event.

A quantitative FTA can be used when the probabilities of primary events are known. Probabilities of occurrence of all intermediate events and the top event (outcome) can then be calculated in accordance with the model. Also, the quantitative FTA is very useful in reliability analysis of a product or a system in its development.

FTA can be used for analysis of systems with complex interactions between sub-systems including software/hardware interactions.

5.2 Objectives

FTA may be undertaken independently of, or in conjunction with, other reliability analyses. Objectives include:

– identification of the causes or combinations of causes leading to the top event;

– determination of whether a particular system reliability measure meets a stated requirement;

– determination of which potential failure mode(s) or factor(s) would be the highest contributor to the system probability of failure (unreliability) or unavailability, when a system is repairable, for identifying possible system reliability improvements;

– analysis and comparison of various design alternatives to improve system reliability;

– demonstration that assumptions made in other analyses (such as Markov and FMEA) are valid;

– identification of potential failure modes that might cause a safety issue, evaluation of corresponding probability of occurrence and possibility of mitigation;

– identification of common events (e.g. the middle branch of a bridge circuit, see Figure 10);

– search for an event or combinations of events which are the most likely to cause the top event to occur;

– assessment of the impact of the occurrence of a primary event on the probability of the top event;

– calculation of event probabilities;

– calculation of availabilities and failure rates of system or its components represented by a fault tree, if a steady state can be postulated, and eventual repairs are independent of each other (same limitation as for the success path diagram/reliability block diagram).

5.3 Applications

FTA is particularly suited to the analysis of systems comprising several functionally related or dependent subsystems. Benefits of FTA are apparent when a system design is the product of several independent specialized technical design groups and the separate fault trees are linked together. Fault tree analysis is commonly applied when designing nuclear power generating stations, transportation systems, communication systems, chemical and other industrial processes, railway systems, home entertainment systems, medical systems, computer systems, etc. Fault tree analysis is also of particular value when applied to systems comprising various component types and their interaction (mechanical, electronic and software components), which cannot be easily modelled with other techniques. An example of this would be a combination of events where their order of appearance is essential such as existence of vibration fatigue causing fracture cracks and failures of components.

FTA has a multitude of uses as a tool (to list a few):

– to determine the pertinent logic combination of events leading to the top event and, potentially, their prioritization;

– to investigate a system under development and anticipate and prevent, or mitigate, potential cause(s) of undesired top event;

– to analyze a system, determine its reliability, identify the major contributors to its un-reliability and evaluate the design changes;
– to assist probabilistic risk assessment efforts.

FTA can be applied to all new or modified products in all design phases, as an analytical tool for identification of potential design problems, including those early phases where information on the design details is incomplete. Those early efforts would then be extended as more information on the system design and its components becomes available. FTA also identifies potential problems that may originate from the product's physical design, environmental or operational stresses, flaws in product manufacturing processes and from operational and maintenance procedures.

5.4 Combinations with other reliability analysis techniques

5.4.1 Combination of FTA and failure modes and effects analysis (FMEA)

This analysis combination is often recommended by sector specific standards, in particular safety standards and transportation standards. The benefits of a combined analysis are the following:

– FTA is a top-down and FMEA a bottom-up analysis method and use of both deductive and inductive reasoning is regarded as a good argument for providing assurance for the completeness of an analysis;
– safety standards often demand a single failure and, in some cases, a multiple failure analysis, the first requirement being fulfilled by FMEA. Both single and multiple failure analysis are accomplished by FTA;
– FMEA is also a useful method for a comprehensive identification of basic events or hazards, while FTA is a practical method for causal analysis of the undesirable events.

Additionally there exists a simple consistency check between FMEA and FTA:

– any identified single failure in FMEA leading to the top event of the fault tree also has to appear as a single point failure (in the minimal cut set);

NOTE A single point failure is a failure that, if it occurs, would cause the entire system to fail.

– any single point failure identified in the FTA should also appear as such in the FMEA.

The value of this consistency check is increased if the analyses are performed separately and independently. This is especially important in safety analyses.

The IEC standard which explains this methodology is IEC 60300-3-1.

5.4.2 Combination of FTA and event tree analysis (ETA)

Any event could be analysed by FTA. However, in some cases this may be not appropriate for several reasons:

– it is sometimes easier to develop event sequences rather than causal relationships;
– the resulting tree may become very large;
– there are often separate teams dealing with different parts of the analysis.