IEC 61025

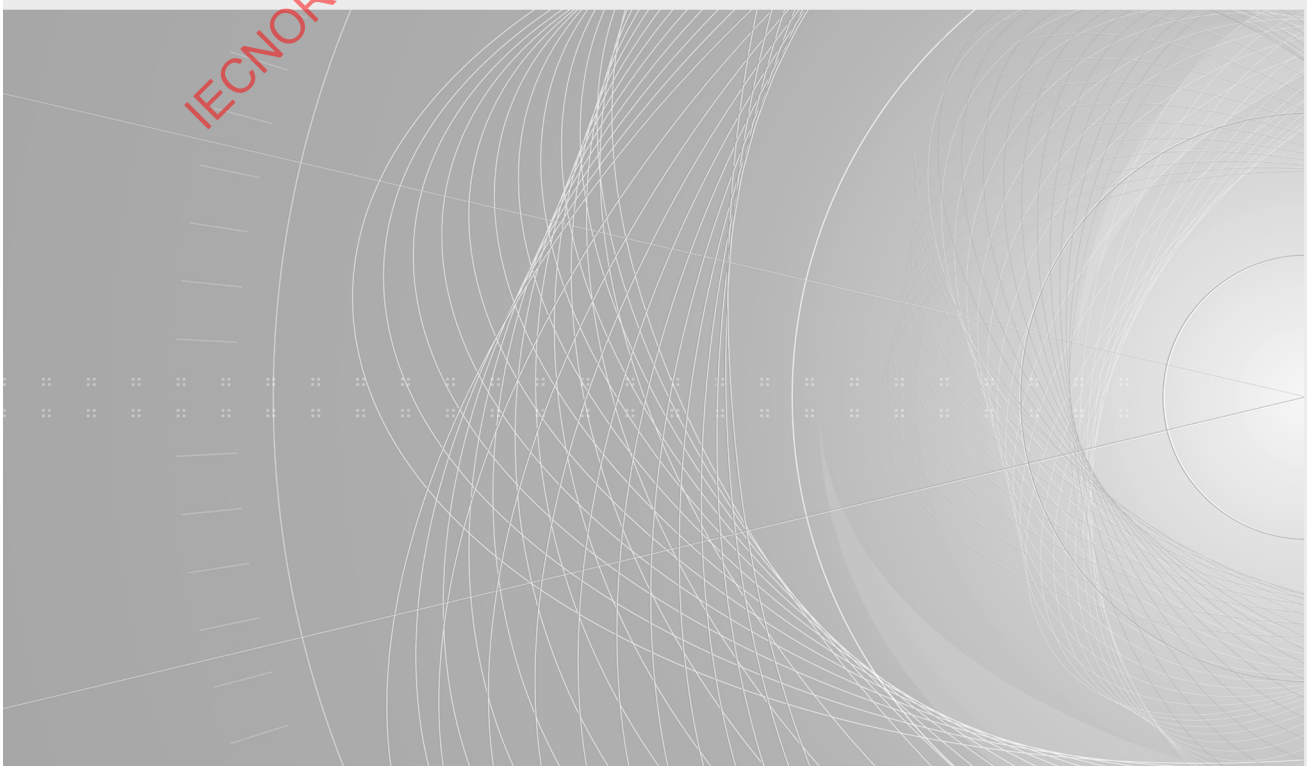
Edition 2.0 2006-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Fault tree analysis (FTA)

Analyse par arbre de panne (AAP)



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 It also gives information on projects, withdrawn and replaced publications.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
CODE PRIX XA

ICS 03.120.01; 03.120.99

ISBN 2-8318-8918-9

CONTENTS

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.

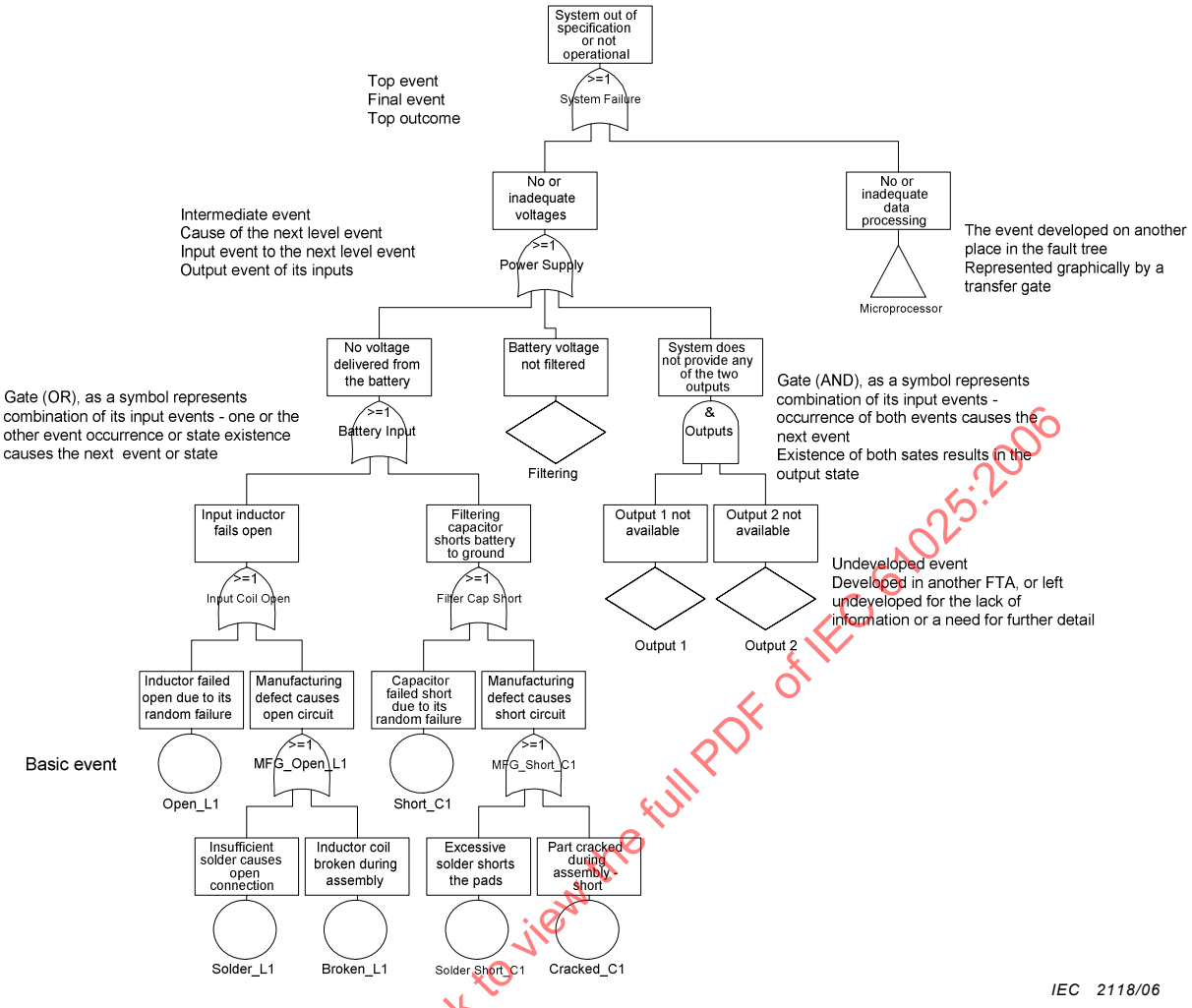


Figure 1 – Explanation of terms used in fault tree analyses

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 of 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.

In order to find a practical procedure, it is often not the top undesired event that is defined first, but potentially undesirable events at the interface between the functional and technical domain.

To give an illustration, consider the top event “loss of crew or vehicle” for a spacecraft mission. Instead of building a large fault tree based on “loss of crew or vehicle,” intermediate undesired events like “ignition fails” or “thrust failure” may be defined as top events and analysed as separate fault trees. These reduced top events would then, in turn, be used as inputs to an event tree in order to analyse operational consequences.

This combination of ETA and FTA is sometimes referred to as cause-consequence analysis (CCA).

5.4.3 Combination of FTA and Markov analysis

FTA that has only a combination of static events (timing – sequencing of the event combination is not considered or modelled – static gates) usually evaluates systems with no sequence dependency of events. However, it is possible to extend the FTA by defining additional gates that represent Markov models. These gates bear the name of “dynamic” gates and include PRIORITY AND gates, SEQUENTIAL gates, and SPARE gates. For such gates, it is necessary to evaluate the failure probability at a time t by using the appropriate Markov model or simulation. Once evaluated, the dynamic gate and its inputs may be replaced by a single primary event, with the probability of occurrence calculated by Markov analysis. Some commercial software allow for modelling of dynamic gates and the capability for calculation of probability of occurrence of the event they represent. An example of dynamic, PRIORITY AND gate is shown in Annex A.

Both static and dynamic gates of a fault tree are used, based on the assumption that the individual events are independent (unless defined as common). However, particular attention shall be given to independence properties between the events included in the Markov model and the events in the fault tree.

5.4.4 Combination of FTA and binary decision diagram (BDD) techniques

Calculation of the probability of occurrence for the top event of a fault tree with many cut sets requires calculation of probability for all cut set combinations. Because of its high complexity, this calculation will often need to be truncated. A BDD may be constructed recursively from a fault tree and it provides an efficient, exact calculation method. This method is well explained in the “NASA Fault Tree Handbook with Aerospace Applications version 1.1[1][1]”.

The BDD approach is useful where truncation of cut set probability calculations results in either unacceptable loss of accuracy or an FTA solution takes excessive time, particularly when many high-probability events appear in the model. Because the minimal paths generated in the BDD approach are disjointed (see 7.5.5.4), calculation of importance and sensitivities can also be performed efficiently and exactly.

1 Figures in square brackets refer to the bibliography.

5.4.5 Combination with the reliability block diagram

A reliability block diagram is made up of blocks or modules, representing a group of components, or failure modes. Those groups are normally formed following the functional block diagram of a product, system or a process. These modules have either a determined failure rate, or a calculated reliability or probability of failure for given use or operational profile. Traditionally, the blocks would have a failure rate which would be the sum of failure rates of individual components. In that manner, the functional interaction of components within a module is not considered.

To augment correctness of functional modelling within a block (software/hardware, interaction of mechanical parts), reliability of certain blocks can be modelled with a fault tree, and then the resultant information on probability of occurrence of those blocks can be assigned to that specific block being part of a reliability block diagram. In this manner, reliability block diagrams, which normally assume independency of components failure within a block, would yield a more realistic prediction.

6 Development and evaluation

6.1 General considerations

6.1.1 Overview

A fault tree is an organized graphical representation of the conditions that cause, or contribute to, the occurrence of a defined undesirable outcome, referred to as the "top event". The representation is in a form that can be clearly understood, analysed and, as necessary, rearranged to facilitate the identification of:

– factors affecting the reliability and other performance characteristics of the system. These factors, for example, include design deficiencies, environmental or operational stresses, component fault modes, operator mistakes, software faults;

– common events that may contribute to more than one outcome of intermediate events in a fault tree. As an example, 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.

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, Method A, or quantitative, Method B, depending on the scope of the analyses.

In cases where the probability of occurrence of the basic events cannot be estimated, a qualitative FTA, Method A, may be used to investigate causes of potential unfavorable outcomes with individual basic events marked with descriptive likelihood of occurrence such as: “highly probable”, “very probable” “medium probability”, “remote probability”, etc. as explained in 5.1.

A quantitative FTA, Method B, can be used when the probabilities of basic or primary events are known. Probabilities of occurrence of all intermediate events and the top event (outcome) can then be calculated using the appropriate mathematical expressions.

6.1.2 Concepts and combinations of events and states

The final outcome of a fault tree (top event) can be a fault in itself, or an event. Here, the fault tree describes a fault or an event resulting from the contributing events or other faults. In the fault tree analysis certain combination of events can be either states or events, while the others must match the outcome. For example, the inputs into an OR gate where the outcome is a state or an event, can be states or events. All inputs into an AND gate which as an outcome is an event must be events, while if as the outcome it represent a state all the inputs must be states.

The state can be characterized by the probability that the state will exist in time *t*, while the event can be characterized either by the failure rate or failure frequency, or by probability of event occurrence at time *t*.

6.1.3 Fault tree for investigation of faults leading to other faults or events

Traditionally, a fault tree is constructed to investigate faults or events leading to an outcome. This concept has been used for a long time in many industries, and is specifically efficient and applied in the nuclear industry. In this manner, it is a powerful and invaluable tool for investigation of potential problems, events, improvements and other preventive measures that preclude or mitigate an undesirable outcome.

An outcome, success or fault, is investigated, and the states or events leading to this outcome investigated, their probability of existence or occurrence determined, and the fault tree model constructed appropriately that would lead to the probability of existence or occurrence of the assumed outcome.

In this application, the fault tree is constructed and evaluated as described in Clause 7, having in mind that the outcome is characterized by probability of fault existence or event occurrence, and is not related to reliability of the analysed item or a system.

It is possible that the basic or any other events in this type of analysis are not given any real probability value, and are only used in investigation of an event that potentially might take place (Method A). In such a case, they might be marked with a descriptive probability of “high, medium, or low”, and are evaluated as potential contributors to the top event or fault. Such types of fault trees are often used for identification of a primary fault or event that was the single or a major contributor to the top fault or event, and are used in a vast variety of industries: automotive, nuclear, manufacturing plants, etc.

6.1.4 FTA use in reliability assessment and improvement during product development

In this application which is based on the FTA Method B, a fault tree can model the entire product, or parts of a product that might pose a risk to its reliability or operational safety. In this case, Method B analysis probability of occurrence can be determined in a traditional manner, such as in analysis of a safety-related fault or event of a product, or the detailed analysis of potential product failure within a certain time period may lead to expression of its unreliability or probability of failure within that period of interest. In this application, the fault tree methodology follows the principles of a top down failure modes and effects analysis, where each potential failure mode may result in an event or a fault leading to the product failure.

The FTA is specifically convenient here as the modelling can reflect the dynamics of events in a product, software/hardware interaction, as well as the interaction between faults or events representing the potential failure modes. This interaction is not possible to represent in a regular FMEA, and is very difficult to model using traditional reliability block diagrams. Also, the product reliability estimates are more realistic, as only the failure modes that contribute to failure of a product, as defined, are considered.

The development of a fault tree should start early in the system design stage and be continued in all of the development stages of a product. The evolution of the fault tree should be such that it reflects the progress of the design. Thus an increased understanding of the failure modes will be obtained as the design proceeds. "Analysis concurrent with design" allows for early systems design change. Many fault trees will be large, in which case fault tree analysis software may be needed to handle them. Software is available to facilitate analysis and allow easy and quick estimates of probability of occurrence of the top event. There are many FTA software programs available and perhaps many more being created. All of them are sufficiently different to suit the needs of a specific use.

It is important to note that fault tree events are not confined solely to software or hardware failures, but include their interaction and other factors, e.g. human factors or actions and processes that are relevant to the top event.

Where quantitative analysis is carried out, but the probability of occurrence of some events cannot be determined, even if the faults or events (failures) are systematic, those events and their functional (logic) combination should be included in the analysis. In this case, these failure modes will not be accounted for in the reliability (or probability of failure) prediction, but their existence is accounted for even in the qualitative manner.

In order to use the fault tree technique effectively as a method for system analysis, the procedure should consist of at least the following steps:

– definition of the scope of the analysis;
– familiarization with the design, functions and operation of the system;
– definition of the top event;
– construction of the fault tree;
– analysis of the fault tree logic;
– reporting on results of the analysis;
– assessment of reliability improvements and trade-offs.

If a numerical analysis is planned, it will be necessary to define a technique for numerical assessment of primary event probabilities or other attributes such as failure intensity, mean time between failures (MTBF) or mean time to failure (MTTF), etc. The selection of the data to be used and numerical evaluation of the reliability or un-reliability measures are outside the scope of this standard.

There are multiple objectives in the FTA of a system design. One of the objectives is to model the product's architecture and functionality in a top-down manner, searching for the potential failure modes and their causes that might produce an outcome as defined by the top event. Based on this information, contributors to the probability of occurrence of the top event or system unreliability (both qualitatively and quantitatively to identify the contributing causes) follow the investigation down in order to identify their respective causes. This allows for trade-off and studies of possible solutions for mitigation of unacceptable potential failure modes, and finally, evaluation of the achieved reliability improvement.

Being a model of a product's architecture and functionality, the FTA should be carried out by personnel with detailed knowledge of the system, its design features and operation, and who are trained in FTA and other relevant reliability modelling techniques. The analyst has to be able to evaluate influences of potential failure modes and logically identify possible causes of abnormal product performance. Lack of engineering knowledge of the product design and potential failure modes will produce an FTA that might not be a true representation of the product functionality and, thus, the analytical results would become meaningless. When prepared, the FTA should be reviewed by the engineering team participating in the product design for correctness and completeness. The corrective actions agreed upon must be documented and followed up.

6.2 Required system information

The system to be analysed should be defined by a description of the system function and by an identification of the system interfaces. Such a definition should include:

– a summary of the design intent;

– a definition of what constitutes the system failure;

– a system functional structure usually represented by a functional block diagram;

– system boundaries, such as electrical, mechanical and operational interfaces, to be governed by the interaction and interfaces with other systems. Such boundaries should be described by identifying the particular functions for example electrical connections (internal or external), fuse, which form the interfaces;

– the physical structure of the system, as opposed to the functional structure;

– an identification of the system operational modes together with a description of system operation and the expected or acceptable system performance in each operational mode;

– a system operational profile;

– the system's environmental conditions, and relevant human aspects (i.e. degree of training for operators and maintenance personnel), etc.;

– a list of applicable documents, for example drawings, specifications, operating manuals, which give details of the equipment design and operation. Task duration, time interval between (periodic) tests, as well as time available for corrective maintenance actions should be known, as should details of the support equipment and personnel involved. Specific information on prescribed functions during each operational phase is also required.

6.3 Fault tree graphical description and structure

Components of a fault tree are as follows:

Gates:

– Symbols showing the logical relationship between input events and the output event
  – static gates – outcome not dependent on the order of occurrence of inputs,
  – dynamic gates – outcome dependent on the order of occurrence of inputs.

A table describing dynamic gates and comments about their use is shown in Annex A, Table A.3. An example of a PAND gate is shown in Figure A.1.

Events

– Lowest level of inputs in a fault tree. Commonly used event symbols and their definitions are shown in Annex A, Table A.1.

Graphical components of a fault tree are as follows:

a) fault tree logic symbol (gates);
b) gate input connection lines;
c) intermediate event descriptions;
d) transfer in or out symbols;
e) primary event symbols.

All relevant events should be included in the fault tree. Such events should include the effects of environmental or other stress conditions to which the item might be subjected including the software, controls and status monitoring; those which are possible during operation, even if outside the design specification.

Events which the analyst has considered, but excluded from further analysis as not applicable, should be documented in the report but not included in the final fault tree.

If the fault tree highlights two or more system performance problems caused by one existing fault, then the event describing that fault should be included in the fault tree in multiple places. This event also should be marked as a common event. In quantitative analysis, the common event is included in calculations only once and all disjointing criteria shown in 7.5.5.4 should be applied. To avoid accidental inclusion of common events in multiple calculations, conventional labelling of such events should be established and used. This type of labelling has to be consistent. If computer software is used for fault tree evaluation assistance, appropriate conventions and settings shall be used.

When fault trees are created, they can be presented in a vertical form, from top to bottom, or in a horizontal form from left to right. When the fault tree is represented in horizontal form, all of the symbols shown in Tables A.1 through Table A.4 are rotated 90° counter clockwise.

The fault trees may also be read or investigated in opposite directions, e.g. dealing with occurred accidents, failures, etc.

7 Fault tree development and evaluation

7.1 General

Development of a fault tree starts with the definition of the top event. Development of a fault tree in its traditional application, or for a system reliability and the failure mode analysis, is a deductive method where the analysis starts from the top undesired event as it is defined for the scope of analysis. Once developed to the intended extent, the fault tree becomes a graphical representation of all events that either by themselves or in conjunction with other events contribute to the occurrence of the top event.

7.2 Scope of analysis

The definition of the scope of analysis should include the definition of the system to be analysed, the purpose and extent of the analysis and the basic assumptions to be made. These assumptions should include those related to the expected operating and maintenance conditions as well as to system performance under all possible conditions of use.

FTA can provide information on

– system reliability analysis, in cases where probabilities of occurrence of the primary events are known,

– the root cause(s) of an unfavourable outcome that has taken place that may require an appropriate corrective action.

FTA scope extends to a complex system when probability of a top event occurring has to be determined. Here, unlike other reliability modelling and prediction analytical methods, the scope of analysis extends to inclusion of only those failure modes or potential events that have influence on the system operation, that is, only those failure modes that are pertinent to the occurrence of the top event. This then results in a more focused system assessment that can be better compared to the field performance.

7.3 System familiarization

In order that a fault tree analysis can be carried out successfully, a detailed knowledge of the system is required. However, some systems may be too complex to be understood fully by one person. In this case, the process of familiarization requires that the necessary specialized knowledge be gathered by team activity.

7.4 Fault tree development

Fault tree development starts with the definition of the top event, or unfavourable outcome which should be defined unambiguously. The top event is the focus of the entire analysis. Such an event may be the onset or existence of a dangerous condition (safety analysis), or the inability of the system to provide a desired performance.

If, in a system performance or reliability analysis, an output event from a gate defines the inability to perform a function, the corresponding input events could represent appropriate causes: e.g. failure due to hardware faults, software faults, performance limitations, incorrect command (control failure) and human error.

The development of a particular fault tree branch terminates after any one or more of the following have been reached:

– primary events, i.e. independent events for which the relevant characteristics can be defined by means other than a fault tree;

– events which need not be developed further, as defined by the analyst;

– events which have been or will be developed further in another fault tree – transfers; if that event is developed further, such an event has to bear the same identification as the corresponding event on the other fault tree so that the latter tree effectively forms a continuation of the former.

7.5 Fault tree construction

7.5.1 Fault tree format

Fault trees may be drawn either vertically or horizontally. If the vertical arrangement is used, the top event should be at the top of the page and the basic events at the bottom. If the horizontal arrangement is used, the top event may be on the left or right of the page.

Examples in the standard (Figure 1 and others) show the development and representation of a fault tree. In addition to the defined symbols for the fault tree logic, the examples contain the event description box, as well as the function or state the event represents.

7.5.2 Use of quantitative (Method B) FTA in system or product development for reliability improvement

7.5.2.1 General

FTA is a systematic manner to identify events that contribute to the occurrence of the top event, and with proceeding deductive methods, to the intermediate events and ultimately to the primary events. This systematic analysis identifies failure modes of system components and the contributing factors to their own probability of occurrence, e.g. operational or environmental stresses including software commands, human factors etc.

The primary difference between FTA and other reliability modelling and analysis methods is that the FTA includes only the events that contribute to the occurrence of the top event, and models their functional combination and possible dynamic interaction and interdependency, while other methods deal with the component failure rates or probabilities (not the component failure mode probability) with the usual assumption of failure independency. As an example, a voltage-filtering capacitor can fail open (about 35 % of its failures), short (about 55 % of its failures) or can change capacitance (the remaining 10% of its failures), but only a failure mode *short* would cause the product failure, then only about 55 % of its failure probability is taken into account. This allows for realistic identification of those failure modes or their causes that need the designer's attention.

Capability of FTA to correctly model sequence of events (with the assistance of Markov analysis) primary or intermediate, as an input into another intermediate event makes it an instrumental tool to identify those primary events/functions or intermediate events that are major contributor to a product's unreliability. This allows design improvements that would mitigate such design flaws, and the revision of the FTA to verify the improvement or to do the trade-off study of two or more improvement options.

In all subsequent gate models, it is important to keep in mind that the probability values are those of failure modes and their contributing factors only, or are the probabilities of the static or dynamic combinations of the failure modes leading to loss of a function and system failure.

The use of FTA in this manner is explained in detail in the “NASA Fault Tree Handbook with Aerospace Applications version 1.1”, mentioned in Clause 6.

7.5.2.2 Series system configuration

In reliability modelling, the assemblies (blocks or components in the reliability block diagram) are in a series configuration in a system when a failure of any of them would constitute the system failure.

The corresponding model in the fault tree would be that all of those “blocks” (gates or events) flow into an OR gate.

The mathematics for reliability of the top “system” consisting of “n” independent blocks would be:

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \cdot .....R_i(t) \cdot ....R_n(t) \quad (1)$$

The above expression in terms of reliability would be that block 1 ***and*** block 2, ***and*** the rest of the blocks have to be operational for the system to be operational.

In FTA, the opposite is used. The failure outcome is produced by either component 1 failure OR component 2 failure, and so on. This is why the OR gate represents a series system or assembly configuration.

The mathematics behind an OR gate is the same as the one shown for a series system, except expressed in terms of probability of failure $F(t)$, which is a probabilistic complement to the reliability.

$$F(t) = 1 - R(t) \quad (2)$$

The probability of an unfavourable outcome of an OR gate (“system”) consisting of n independent input gates or events is:

$$F_S(t) = 1 - (1 - F_1(t)) \cdot (1 - F_2(t)) \cdot ..... \cdot (1 - F_i(t)) \cdot ..... \cdot (1 - F_n(t)) \quad (3)$$

The system fails when any of the components (blocks) fail. An example of an OR gate is shown in Figure 2. In Figure 2, and all subsequent figures in this clause, the relevant failure mode of a component is the failure mode which, as an input event, causes occurrence of the output event.

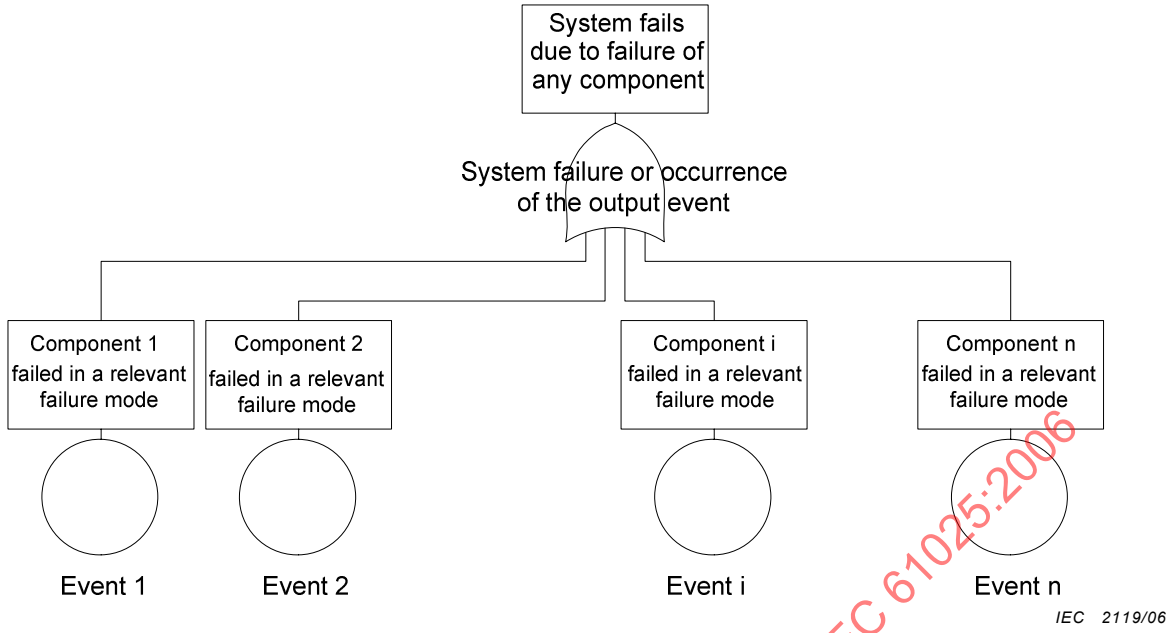


Figure 2 – Fault tree representation of a series structure

7.5.2.3 Parallel system configuration, redundant systems

7.5.2.3.1 Active redundancy

This subclause assumes that failure characteristics (models) for each input to the active redundancy remain the same, independent of how many other inputs are working. It also assumes that each input to the active redundancy block is independent. Where it is not independent, see disjointing (Annex B) for additional guidance.

If an output event were to occur only if all contributing independent events occur, then they should be linked by an AND gate. Such a configuration may be redundant. It is also referred to as a parallel system for reliability analysis, even though the physical configuration might be different.

The independence requirement is met when the probability of input events does not change, regardless of the state of other inputs.

The associated mathematical expression in reliability is that the system is operational if component 1 OR component 2, OR out of any of the components, at least one of them remains operational, that is the system fails if all of the components fail.

$$R_S(t) = 1 - \prod_{i=1}^{n} \left(1 - R_i(t)\right) \tag{4}$$

With the FTA, this is represented by an AND gate, having "n" input gates or events, with the meaning that the system fails if component 1 AND component 2, AND the rest of the components fail, with similar mathematics. The probability of failure is then:

$$F_S(t) = \prod_{i=1}^{n} \left(F_i(t)\right) \tag{5}$$

An FTA representation of parallel redundancy, where only one component surviving is sufficient for the successful system operation, or the system fails only if all components fail, is shown in Figure 3.

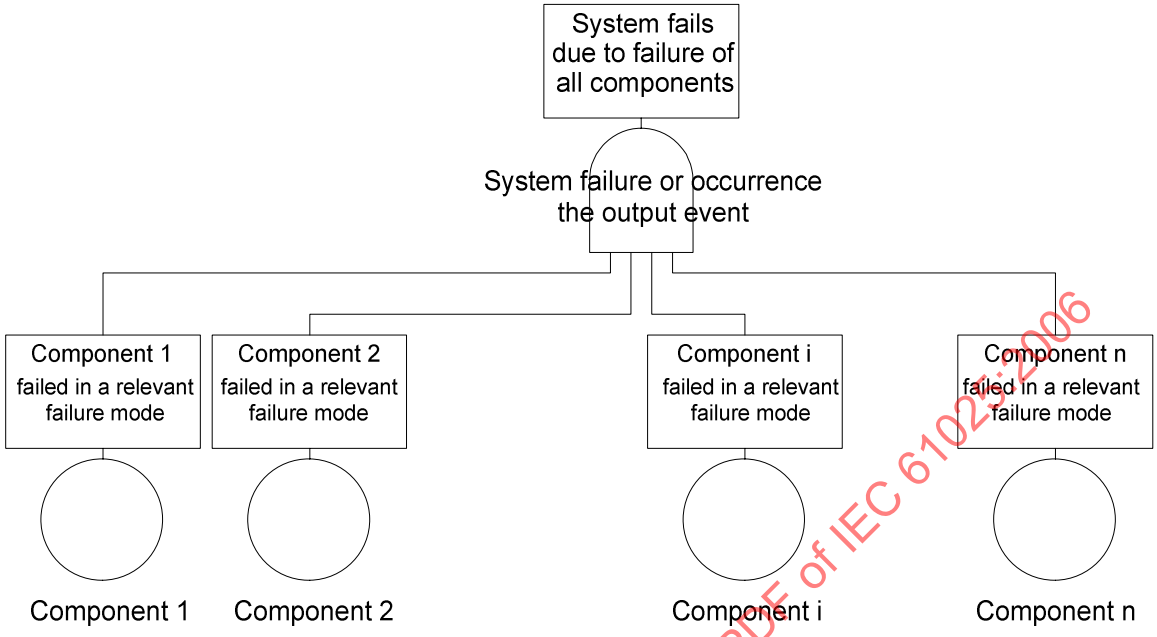


Figure 3 – Fault tree representation of parallel, active redundancy

Redundant components may operate in a load-sharing mode (e.g. generators to a power network), the failure event probability of surviving components may increase as each fails. Such changes in event probability would break the independence requirement for use of a simple AND gate.

If an output were to occur only if all contributing events occur, but the input events are dependent on each other, then an AND gate cannot be used. In that case, a dynamic gate is used.

When the redundancy is such that the condition of system success is that k out of n identical blocks remain operational, then the mathematical expression for unreliability as used in the FTA is as follows:

$$R_S(t) = 1 - \sum_{i=0}^{k-1} \frac{n!}{i!\cdot(n-i)!} \cdot [R_0(t)]^i \cdot [1 - R_0(t)]^{n-i}$$

or (6)

$$F_S(t) = \sum_{i=0}^{k-1} \frac{n!}{i!\cdot(n-i)!} \cdot [1 - F_0(t)]^i \cdot [F_0(t)]^{n-i}$$

In FTA, this combination of events is represented by the majority vote gate, where the vote number is $m = n - k + 1$ and the symbol in the corresponding gate, m, designates how many events have to take place for the event to propagate further in the tree.

As an example, if the required redundancy is 3 out of 6, the majority vote is 4, as the occurrence of four input events would leave only two remaining components operational, which means that the system had failed, as the requirement was for three components to be operational out of 6.

The majority vote gate, along with other examples of gates used in reliability modelling, is shown in Figure 4.

7.5.2.3.2 Passive (stand-by) redundancy

Stand-by redundancy is when only the number of components required for operation is active, and in case of failure of one or more of those components one or more replacement spares is activated to take the function of the failed components. System failure is defined as the event when the total number of functional components is less than the number required for system operation. The redundant components (spares) may in analysis be considered not subject to failure (cold spares) or subject to some intermediate likelihood of failure (warm spares) until brought into the active operation, or may be equally subject to failure as when operational (hot spares).

Representation of stand-by redundancy is not possible with the static gates. However, a SPARE gate symbol may be used. Markov analysis shall be used to analyse this gate.

Stand-by redundancy is successfully addressed by dynamic gates. Here, the SPARE gate is used for redundant systems where event probabilities change.

7.5.2.4 Representation of conditional probability repeated (common cause) events, and transfer out events

Conditional probability is where the probability of an event taking place is dependent on occurrence of another, where the second event takes place only if the first event occurs.

Conditional probability is also expressed in terms of dynamic gates that use Markov state analysis, such as PRIORITY AND gates defined in Table A.4, Annex A.

An example of conditional probability is shown as a part of Figure 4.

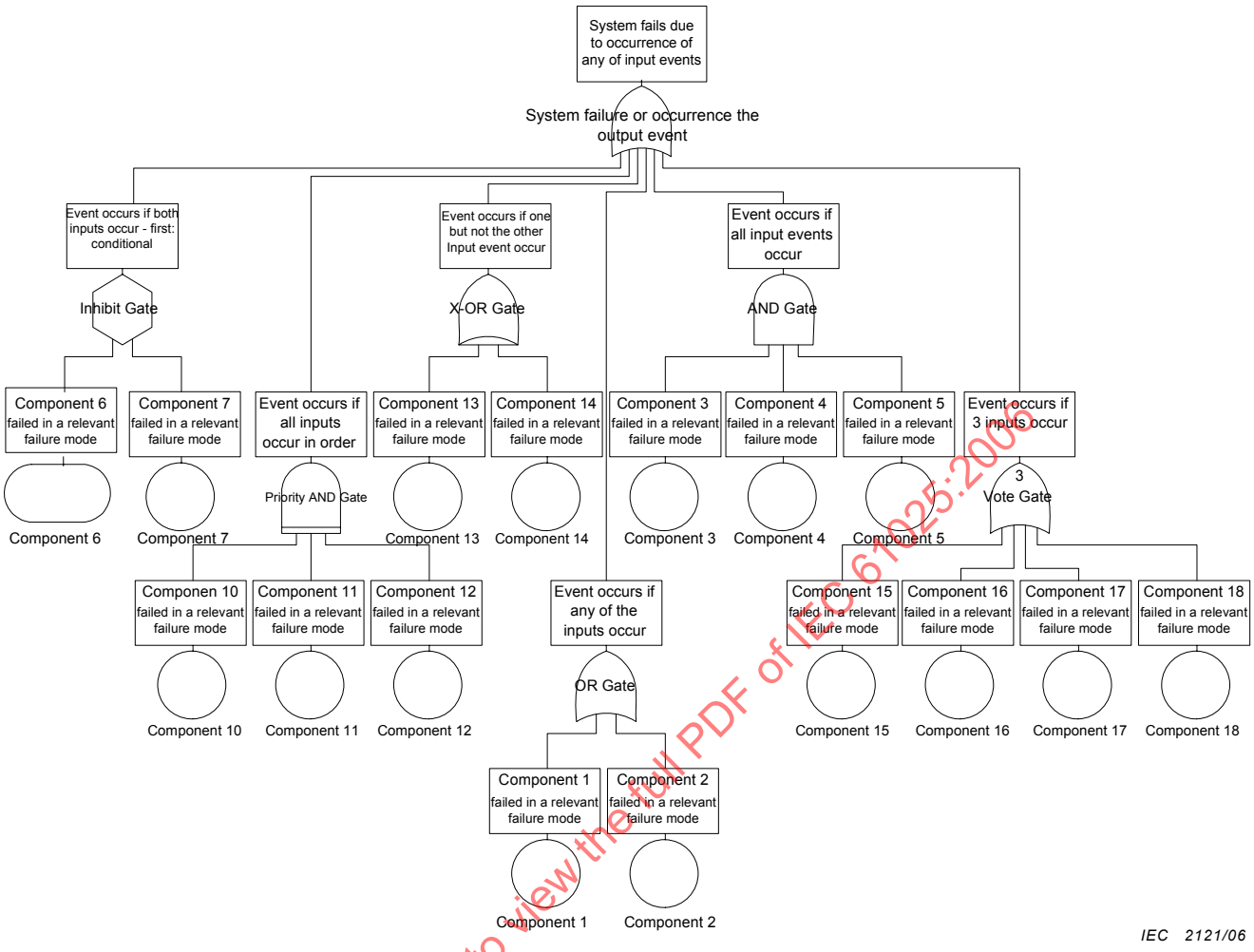


Figure 4 – Example of fault tree showing different gate types

The graphical representation of a fault trees shown in Figure 1 and other figures shown in this standard should be considered examples only.

7.5.2.5 Visual representation of fault trees

Fault trees may have various graphics, dependent on the preferences and customary representation in different countries and in different applications. Some representations use rectangular shapes with the symbols in them such as **&**, for an AND gate, and **≥** for the OR gate. In this case, the null gate is also classified as an OR gate, except such an OR gate has only one input event, as null gates represent an outcome event having only one input event. Caution should be exercised when representing the gates and events as rectangles to ensure that the symbols in them are well defined and clearly marked.

The rectangular gates and events representation is shown in Figure 5.

In Figure 5, event A will occur only if both events B and C occur. Event C occurs if either event D or E occurs.

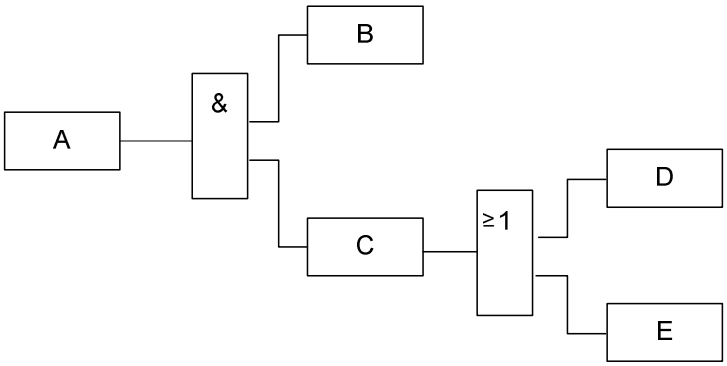


Figure 5 – Rectangular gate and events representation

NOTE For each event, A, B, etc., it is preferable to list the name or description of the event first, followed by event code and probability of occurrence.

If an event represents a repeated event or a common cause event, it is shown in the fault tree repeatedly, but with a flag that it is also shown as an input event to other events in the fault tree. All repeated or common cause events in the set shall have the same event code and be marked by a transfer-in symbol or a symbol normally used as such in a particular fault tree. This rule applies to all repeated or common cause events except the event on the lowest level in the set, which is marked by a transfer-out symbol. In some fault tree graphics, the symbols for the repeated primary events or higher levels, are the same.

Figure 6 shows an example or graphical representation where the repeated event, represented as an OR gate and flagged with the page number, is found in another place of the fault tree, where it is an input event to a different, higher level event. This event can appear in more than two places of a fault tree. An example of such an event could be elevated temperature or humidity causing occurrence of two different events in a system. Disjointing is in this case applied to such event. Also in Figure 6, a transfer gate is shown to indicate that this event was developed in another place or page of a fault tree. This usually is the case when a more complex event is an input event to a higher level event, thus it has to be further developed on a separate sheet. A PRIORITY AND gate, shown in Figure 6, would be used when the output event is dependent on the ordering of input events.

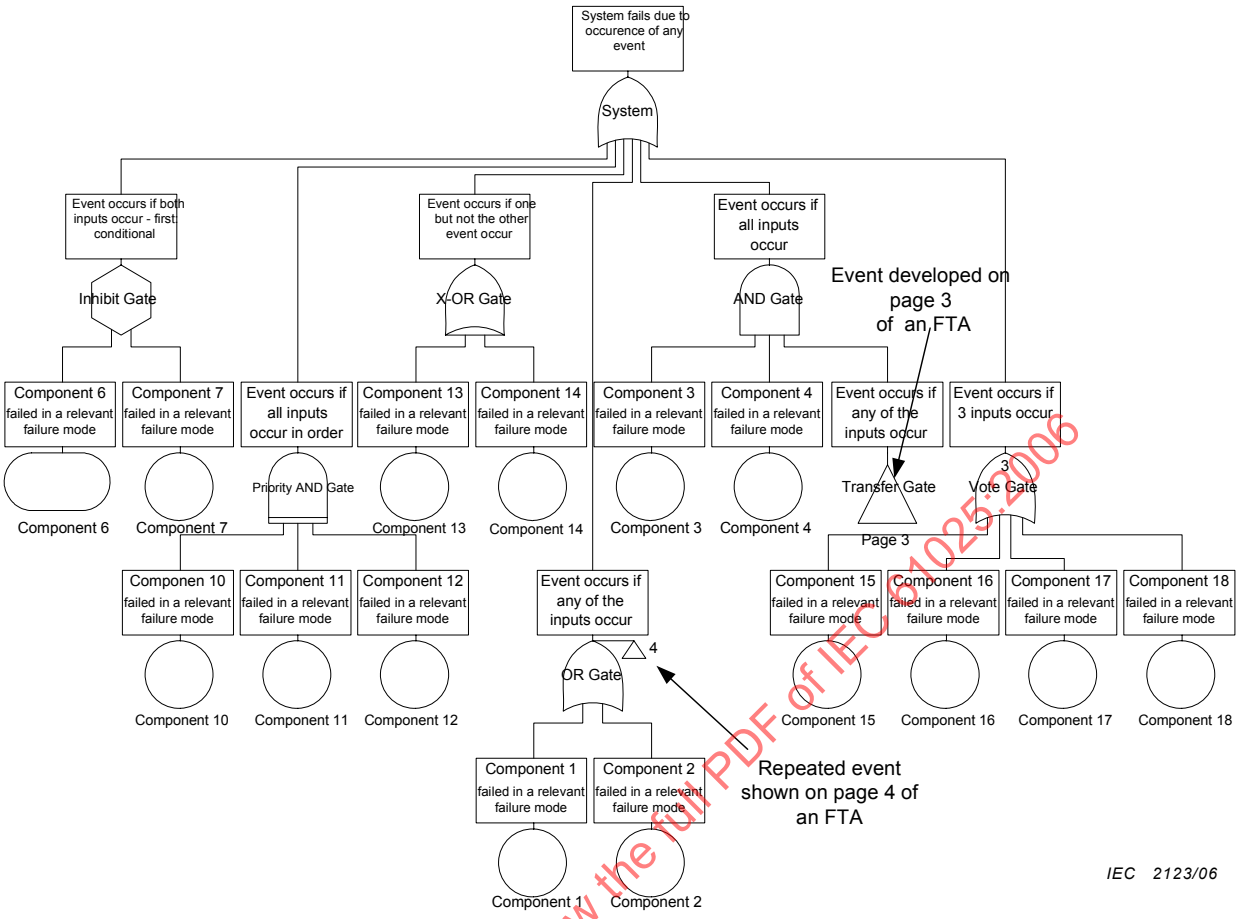


Figure 6 – Example fault tree containing a repeated and a transfer event

An example of a rectangular fault tree showing transfer out repeated or common cause event is shown in Figure 7. Event B is an event, which is analysed further on another fault tree. Event D is a basic event.

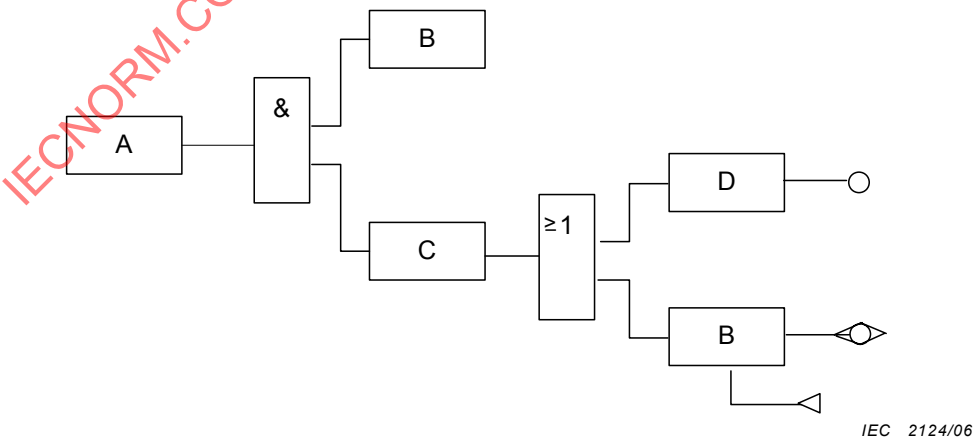


Figure 7 – Example showing common cause considerations in rectangular gate representation

7.5.3 Construction procedure

The first steps in construction of a fault tree is to clearly define the top event, the scope and the objective of the fault tree, the boundaries of the system or object of analysis and the resolution of the analysis. This objective should be defined in terms of the definition of the top event.

The top event must describe a problem that has to be analysed in order to determine contributing causes. In FTA application for reliability improvement of a system under development, the top event is a system failure and the objective of analysis is to determine contributors to this event and identify design weakness or unreliable components. In quantitative analysis the probability of occurrence of the top event and all, or most, inputs will be determined. In qualitative analysis, Method A, the inputs to the top event will be investigated in order to identify the causes of its occurrence (other events or faults). In quantitative analysis, Method B, for design improvement, the inputs to the top event are analysed to identify the major contributors to the top event and to improve design by systematic elimination of those weaknesses or mitigation of contributing failure modes.

The scope of analysis defines the events or the failure modes that will be included in the fault tree. The scope also covers the details of the problem being analysed, the revision level of the system design under analysis and the use profile of the system and other operational and environmental conditions, while the boundaries define what is included and what is excluded from that system (e.g., internal connections, mechanical enclosures, etc.).

A fault tree should be constructed in such way that it clearly represents the flow of events that cause occurrence of the top event.

Once the top event is clearly defined as well as the system boundaries or analysis extent, then the fault tree construction flows from the top down. The top event has inputs and their combination is modelled and represented by the appropriate gate. Inputs into the top event are then developed systematically to be results of their own input events. Each of the inputs, going down the fault tree, is developed separately and this development is completed when the primary events are reached.

The resolution will specify to what extent the system is to be analysed. As an example, an electronic system can be analysed down to its components and their failure modes and causes, or to a higher level of its assemblies (e.g., signal processor, power amplifier, specific supply voltage regulators, etc.). At times, the resolution can be a combination of detailed and assembly level analysis, dependent on availability of probability of occurrence information.

Strict adherence to the concept of "immediate cause" is necessary to ensure that failure modes are not omitted by reason of the assumption that such modes have been included previously.

The concept of "basic units" can be used to save the analyst the effort of developing fault tree diagrams that do not yield new or useful information. A basic unit is not developed further. It is treated as if it were a single unit or component or dealt with separately.

In order for the unit or event to be considered "primary", it is necessary and sufficient that the following three requirements be satisfied:

– both the functional and physical boundaries are clearly defined;

– operation of the unit does not depend on any supporting function, or all events related to the unit are expressed by a single OR gate having one of the inputs representing a fault of the unit, the remaining inputs representing inability to perform the corresponding support functions;

– no immediate causes can be determined for the occurrence of that event.

The nomenclature used in a fault tree should be standardized so as to minimize confusion and to clearly label and explain what the events are in an organized manner.

The actual construction of a fault tree follows the analytical logic of the flow of events.

– The "immediate cause" concept requires that the analyst determine the immediate necessary and sufficient causes for the occurrence of the top event. It should be noted that these are not the basic causes of the top outcome or top event, but the immediate causes or immediate mechanisms for the top event to occur. These may be the lower level (intermediate) events.

– The immediate, necessary and sufficient causes of the top event are now treated as intermediate events, and the analysis continues to determine their immediate and sufficient causes (input events) to determine their necessary and sufficient causes.

– The construction proceeds down the tree, transferring attention from mechanism to mode, and continually approaching a lower level of mechanism and mode, until ultimately the appropriate or defined level of resolution is reached. The individual basic events or primary (bottom) events are those that represent individual causes of potential failures or faults.

7.5.4 Fault tree evaluation

7.5.4.1 Investigation and analysis

Investigation includes a review of the fault tree structure by comparison with available information such as schematics, drawings, functional diagrams, software commands, identification of common events and a search for independent branches. Investigation should identify common cause events, but should not assume that their presence is benign. Such conclusions can be drawn only after a thorough analysis, using Boolean reduction or determination of minimal cut sets when the static gates are present, as the cut sets do not exist in dynamic gates, unless approximation is applied to ignore sequencing. As the difficulty of the analysis increases rapidly with the size of the fault tree, inspection of the fault tree allows the analyst to identify which branches of the fault tree are independent and can thus be analysed separately if needed.

Analysis of a fault tree follows the flow of events and identifies the causes of those events downward. Fault tree evaluation may be either logical (qualitative) or numerical (quantitative) or both. Analysis of a quantitative fault tree used in product development for reliability improvement identifies the high contributors to the probability of occurrence of the top event, and the causes for those with a high probability of occurrence. As an example, if the probability of failure of an assembly of a system is a high contributor to the probability of system failure, the cause is investigated and once identified, that failure mode can be mitigated. To illustrate this example, a high contributor to the probability of a failure of a system power supply can be identified as an overstressed capacitor. Replacement of that capacitor with another, with higher voltage rating, considerably reduces probability of failure of the assembly and subsequently of the system.

Analyses should be documented in such a way that results can be reviewed and any changes needed can be incorporated in order to reflect changes in design, operating procedures or improved understanding of the physics of failure. In order that this may be done, a systematic approach to the construction is required. To implement this systematic approach, two concepts have to be understood and used consistently. These are the concepts of "immediate cause" (input events) and of "basic unit".

The primary purposes of logical (qualitative) and numerical (quantitative) analyses of a system can be summarized as follows:

– identification of events or faults which can directly cause a system failure, and contribute to the probability of such events and, in that manner, improve dependability (reliability) of a system;
– mitigation of faults that may be contributors to the outcomes that may be potential safety hazards;
– assessment of fault tolerance of the system (ability to function even after a specified number of lower level failures or events contributing to the occurrence of a system failure have happened);
– assessment of information to locate critical components and failure mechanisms;
– identification of device failure diagnostics, inputs to repair and maintenance strategies, etc.

The assessment of fault tolerance of the system includes a determination of the degree of redundancy in the system and a verification that the redundancy is not impaired through common events. Although the major part of fault tolerance assessment does not require the use of numerical data, such numerical data are required to evaluate which combinations of events causing a system fault are the most likely to occur.

7.5.4.2 Logical analysis

7.5.4.2.1 General

Three basic techniques are used for logical analysis: investigation, Boolean reduction and determination of minimal cut sets. The basis of logical analysis is modelling which provides fault tree representation of a structure, be it functional, architectural, or a mixture of the two. Correct modelling means representing the functions or components of a system in such a way as to establish their interactions, dependencies, immediate causes of unfavourable outcomes, etc.

7.5.4.2.2 Boolean reduction

Boolean reduction can be used for the evaluation of the effects of common events (identical events occurring in different branches) in fault trees where the occurrence of the top event does not depend on timing or sequencing of events. Boolean reduction can be carried out by solving Boolean equations for the fault tree. Boolean reduction can also be used to identify minimal cut sets.

7.5.4.2.3 Identification of minimal cut sets

There are several methods of determining minimal cut sets, but application of larger trees may be difficult and incomplete. For this reason, various computer programs are available to assist the analyst.

A cut set is a group of events which, when occurring together, cause the top event to happen. A minimal cut set is the smallest such group in which all events have to occur for the top event to occur. If any of the events in a minimal cut set does not occur, the top event will not occur. The definition can be extended to fault trees dependent on sequencing of events. In such instances, the minimal cut set determines the group of events with the potential to cause the top event. When the occurrence of the top event depends on the sequence of the input events, this event is analysed using Markov techniques which are described in IEC 61165.

7.5.4.3 Numerical analysis

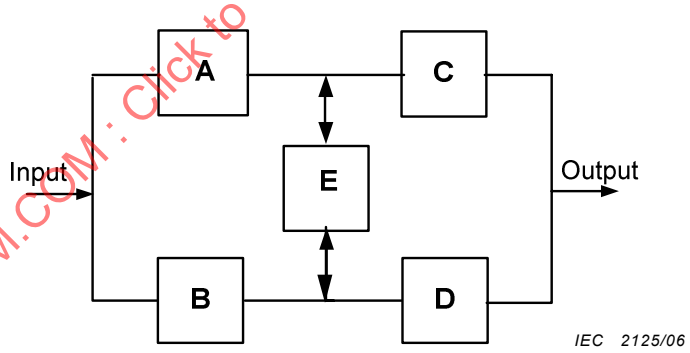
The purpose of numerical analysis is to provide a quantitative assessment of the probability of occurrence of the top event or a selected set of events. Numerical analysis can also be used to support and supplement logical analysis. In order to perform a numerical evaluation of a fault tree, probabilistic data at the component level are required. Reliability and availability prediction techniques, actual test or field use data may be used to establish the quantitative values.

7.5.5 Examples of a simple hardware evaluation using Boolean algebra and its representation by a fault tree

7.5.5.1 Bridge circuit example

Fault tree with Boolean algebra can simplify reliability analysis. As shown in this example, the very complex mathematical expressions that would have to be written if the analysis was done using the reliability block diagram, are substituted by considerably easier Boolean algebra. Understandably, the use of FTA is especially convenient for the more complex circuits where there is also interdependency of software and hardware, and analysis is done using one of many available software packages.

An example of use of the fault tree analysis for representation of a bridge circuit is shown in Figure 8.



NOTE See Figures 11 and 12 for equivalent fault trees.

Figure 8 – Bridge circuit example to be analysed by a fault tree

In the bridge circuit above, the signal has to flow from **Input** to **Output**. It can flow through block E in both directions. One way to perform analysis would be to model the system under two possible circumstances, first assuming that block E is good, and secondly assuming that block E is bad. In the first case, the signal would flow through blocks A or B and C or D, as if they were parallel blocks, respectively. When block E is bad (the condition that E failed), blocks A and C are in series, parallel to blocks B and D also in series. This is represented by the following equation:

$$R_S = (R_A + R_B - R_A \cdot R_B) \cdot (R_C + R_D - R_C \cdot R_D) \cdot R_E + (R_A \cdot R_C + R_B \cdot R_D - R_A \cdot R_B \cdot R_C \cdot R_D) \cdot (1 - R_E) \quad (7)$$

If: $R_A = 0{,}78;\ R_B = 0{,}30;\ R_C = 0{,}15;\ R_D = 0{,}50;\ R_E = 0{,}40$

then: $R_S = 0{,}344$

Probability of failure would then be:

$$F_S = 0{,}656$$

Bridge circuit (system) fault tree representation is shown in Figure 9.

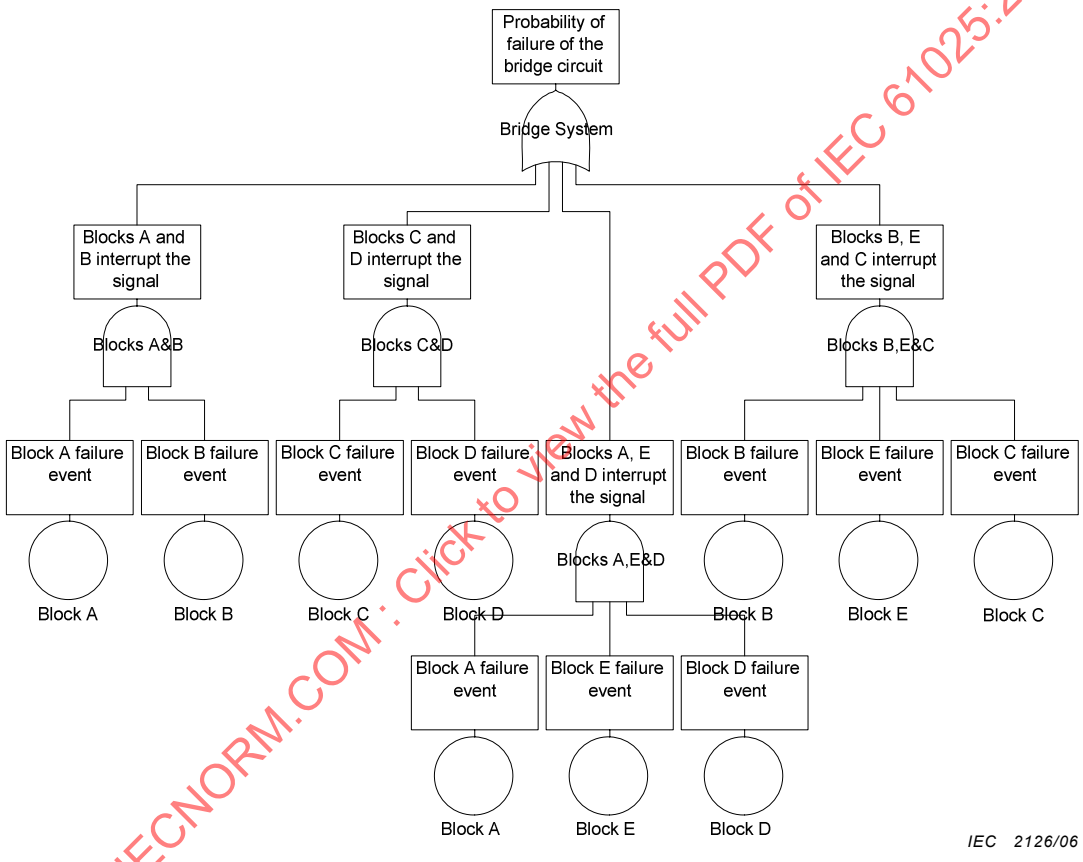


Figure 9 – Fault tree representation of the bridge circuit

Using Boolean algebra, and the minimal cut sets (paths that would prevent system operation) the system in Figure 9 becomes as follows:

Cut sets in this system would be made of the following event combinations of the signal blocking through:

– blocks A and B (c_1 = F_aF_b= ab);
– blocks C and D (c_2 = cd);
– blocks A, E and D (c_3 = aed);
– blocks B, E and C (c_4 = bec).

Should any of the above combinations occur, the signal flow from 'In' to 'Out' will be interrupted.

With Boolean algebra, the probability of the system failure would be:

$$F_S = \Pr(c_1 \cup c_2 \cup c_3 \cup c_4) \tag{8}$$

Probabilities of the cut sets are

$$\begin{aligned}
&\Pr(c_1) = F_A \cdot F_B = (1 - R_A) \cdot (1 - R_B) \\
&\Pr(c_2) = F_C \cdot F_D = (1 - R_C) \cdot (1 - R_D) \\
&\Pr(c_3) = F_A \cdot F_E \cdot F_D = (1 - R_A) \cdot (1 - R_E) \cdot (1 - R_D) \\
&\Pr(c_4) = F_B \cdot F_E \cdot F_C = (1 - R_B) \cdot (1 - R_E) \cdot (1 - R_C)
\end{aligned} \tag{9}$$

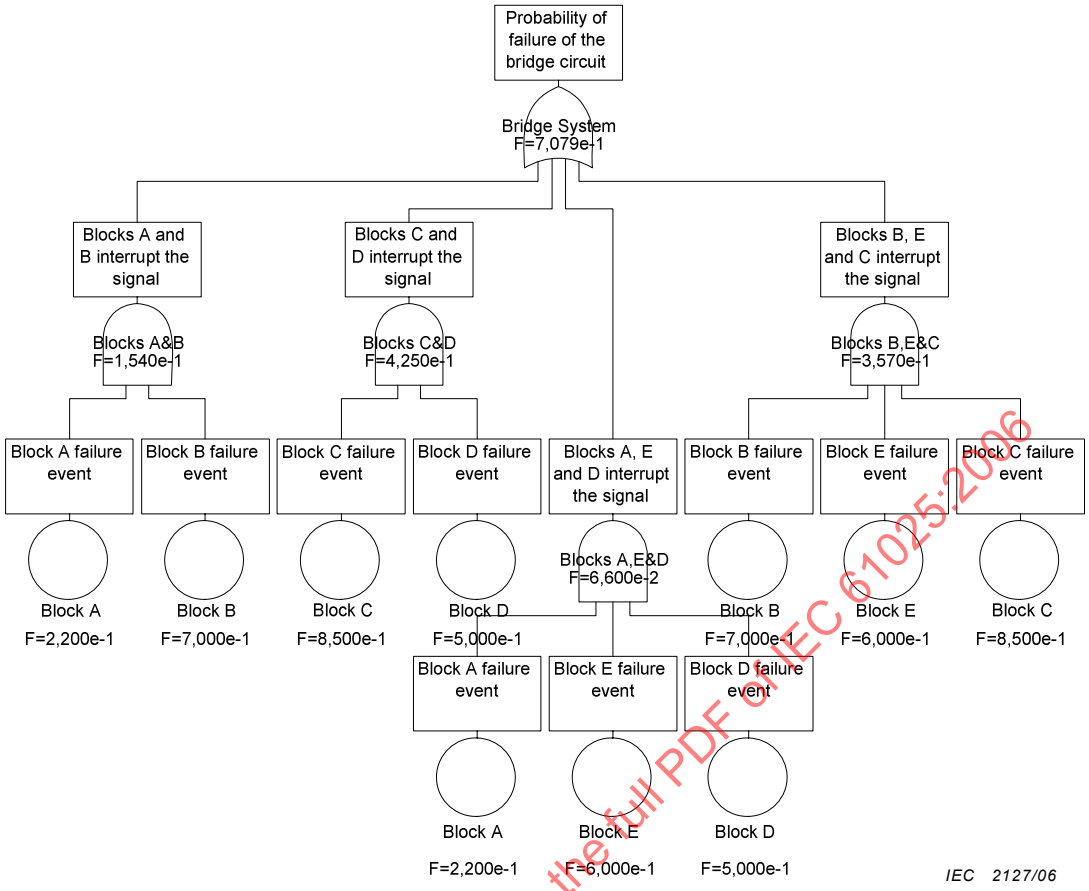
The above simple example has the assigned probability of deliberately large failure numbers in order to illustrate the correctness of some fault tree or Boolean algebra calculation methods, and point out the errors that can be introduced by other calculation methods. These errors might occur in large fault trees prepared for systems even though the probabilities of occurrence of primary or basic events are very small. The probability of occurrence of events of such large fault trees roll up into the higher levels, so that the input events in the top event may have a high probability of failure, causing the incorrect results in the estimate of the probability of occurrence of the top event.

7.5.5.2 Esary-Proschan method

Without taking into consideration the common branch that should not be included more than once in the calculations, the probability of failure (without disjointing) in accordance with Esary-Proschan equations would be (without disjointing):

$$\begin{aligned}
&F_{S-EP} = \Pr(c_1 \cup c_2 \cup c_3 \cup c_4) = \\
&1 - [1 - \Pr(c_1)] \cdot [1 - \Pr(c_2)] \cdot [1 - \Pr(c_3)] \cdot [1 - \Pr(c_4)] \\
&F_{S-EP} = 0{,}7079 \\
&R_{S-EP} = 0{,}2921
\end{aligned} \tag{10}$$

The above calculations are represented by the fault tree shown in Figure 10 where the option for disjointing is not used.



NOTE This is not a fully accurate calculation.

Figure 10 – Bridge system FTA – Esary-Proschan, no disjointing

7.5.5.3 Rare-event calculation

Rare-event approximation ignores all likelihood of concurrency of cut set occurrence. With rare-event approximation, this calculation (again disregarding disjointing), the probability of failure and reliability of the same system would be a simple addition of probability:

$$
\begin{aligned}
F_{S-RA} &= \Pr(c_1) + \Pr(c_2) + \Pr(c_3) + \Pr(c_4) \\
F_{S-RA} &= F_A \cdot F_B + F_C \cdot F_D + F_A \cdot F_E \cdot F_D + F_B \cdot F_E \cdot F_C \\
F_{S-RA} &= 1{,}002 \\
R_{S-RA} &= -2 \cdot 10^{-3}
\end{aligned}
\qquad (11)
$$

While easy to implement, rare-event approximation may introduce sizeable errors into calculations when the failure probabilities are larger numbers as seen on the above example (note probability of failure higher than unity).

Rare approximation represented and calculated with the FTA is shown in Figure 11.

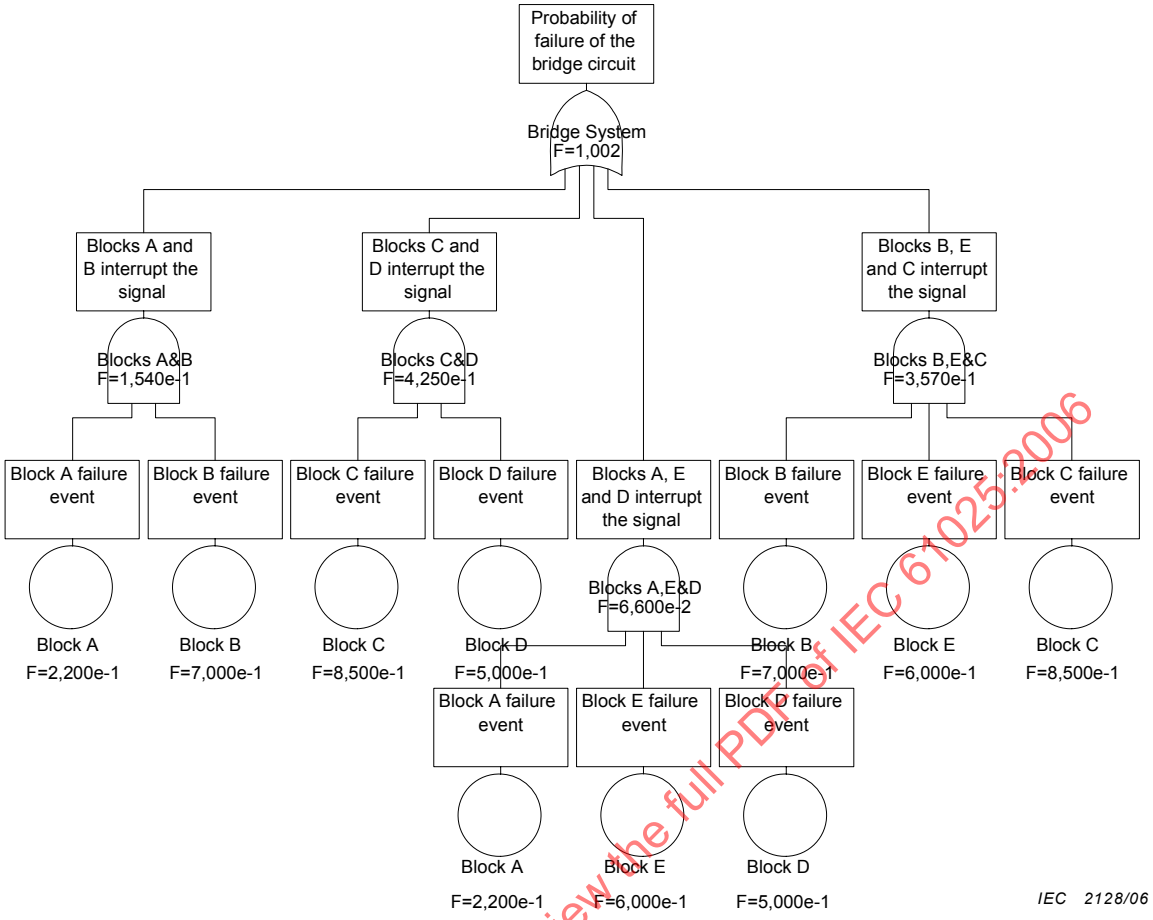


Figure 11 – Bridge system probability of failure calculated with rare-event approximation

As seen in Figure 11, when probabilities of failure of input events are considerably large numbers, which is often the case with the input events to the top event of a large system, a serious error in calculation might result (observe that probability of occurrence of the top event is erroneously declared to be greater than unity).

7.5.5.4 Disjointing

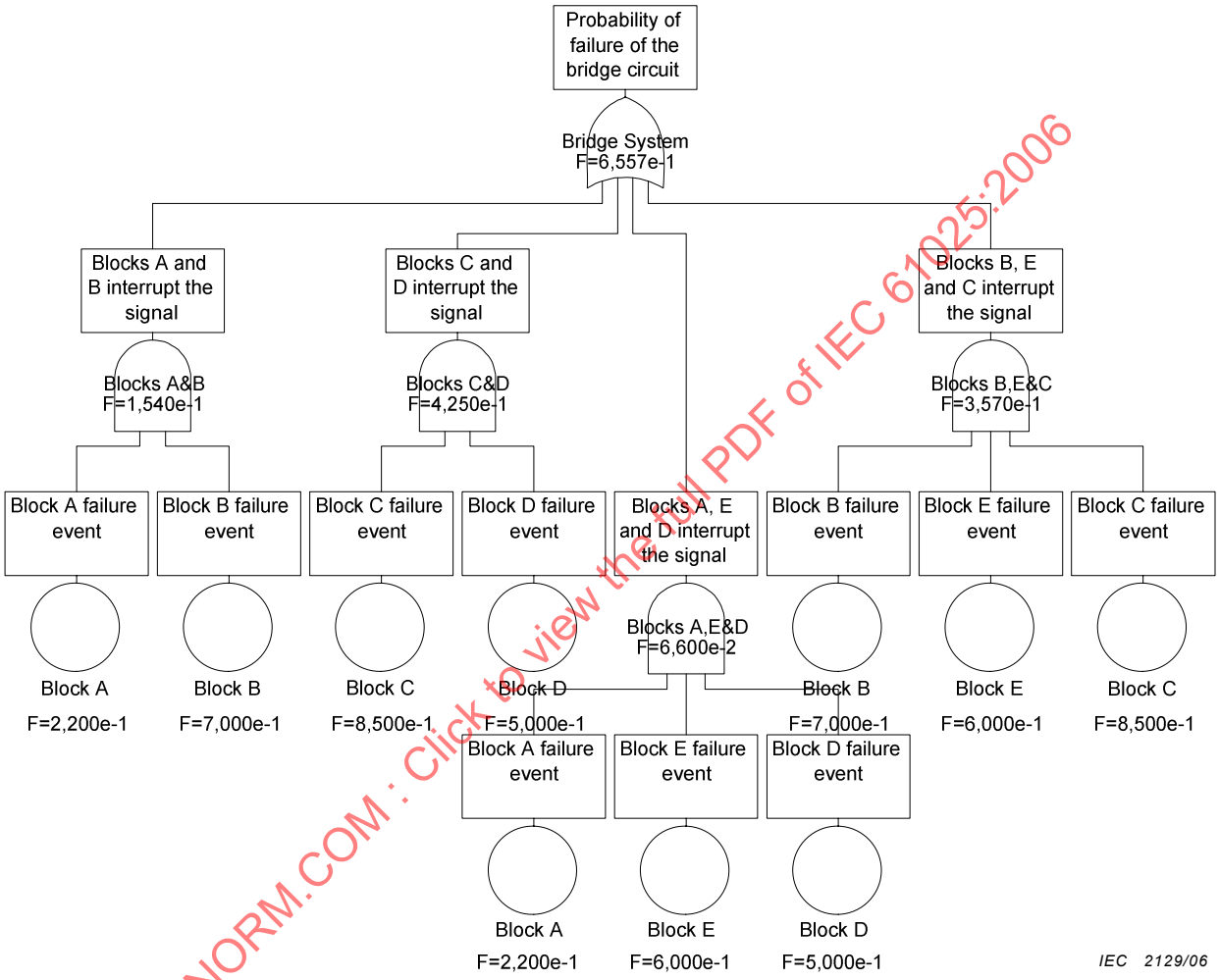
Disjointing is a series of algebraic operations to ensure that the common branch (or common cause failure) does not get included into calculations repeatedly. There are several methods available for disjointing: algebraic, multiple steps where, with multiple terms present in calculations, the terms are disjointed from previous terms; beta factor model, alpha factor model, multiple Greek letter model, etc. All but the first are used for calculating common cause failures.

Disjointing is explained in detail in Annex B.

It is important to note that disjointing procedures can be written as a computer program. By using such a program, quite formidable Boolean expressions can be easily disjointed. This leaves the reliability practitioner free to concentrate on getting a correct expression for system success (or system failure). The tedium of converting the Boolean expression to a probabilistic reliability expression is then left to the computer.

The approach using the theorem of total probability on the other hand, works exceptionally well for the example chosen, but can become quite complicated in many instances, especially when the RBD is asymmetrical.

Many FTA commercially available software packages contain an option for disjointing. Figure 13 shows the calculations when disjointing is enabled. This figure is drawn disregarding any specific software, as this standard refrains from recommendations or software preferences. These are left to the users in accordance with their specific needs



NOTE This is a fully accurate calculation.

Figure 12 – Probability of occurrence of the top event with disjointing

In Figure 12, for the system reliability or the complement, the top event probability of occurrence is the same as calculated using the first reliability modelling equation.

In Figures 10, 11 and 12, symbol F stands for probability of failure for a non-repairable system.

7.6 Failure rates in fault tree analysis

In many instances, the fault tree analysis can use failure rates instead of failure probabilities of events. In this case, the assumption is that Poisson distribution is applicable to characterize occurrence of events, and that the associate failure rates are constant. The algebra used in this case relates to conventional reliability modelling, and the algorithms used for the calculation of failure rates of the output events are the same used in reliability block diagram modelling. The resultant top event is also represented by its failure rate.

It is also possible to construct a fault tree with a mixture of failure rates and failure probabilities assigned to various events. The easiest way to analyse this type of fault tree is to convert failure rates into respective probabilities of occurrence and apply standard fault tree analysis principles. Some software does accept mixed information on events, and uses appropriate algorithms to provide the probability or a failure rate of the top event. In this case, additional information needed is the time interval for which the probabilities of failures are considered.

Expanded use of the FTA for analysis of repairable systems is a separate topic and not part of this standard.

8 Identification and labelling in a fault tree

Each event in the fault tree shall be uniquely identified. Events should be labelled so that cross-reference from the fault tree to the corresponding design documentation can easily be made.

The top event of the fault tree is the undesirable outcome, which is the primary reason for undertaking the fault tree analysis. It should be noted that only a single top event may be associated with a given fault tree.

If several events in a fault tree all refer to different failure modes of the same item, then such events shall be labelled so as to enable them to be distinguished. At the same time it should be clear that they are a group of events related to the same item. Most of the software packages for the FTA will not allow the analyst to label two input events with the same name, thus forcing the analyst to consciously assign the same name to the repeated events and to common cause events.

If a particular event such as inability of a particular valve to close, occurs in several places in a tree, or if it occurs in several trees, all such occurrences shall bear the same label (using software, the same input event will be appended with its specific name to different places in the fault tree). However, events which are similar but which involve different items shall not bear the same identification.

A typical event code should contain information relating to the subsystem identification, for identification of a component and its failure mode (second bullet below).

Some examples from electronic circuit analysis are as follows:

– “Short_C132”, meaning that the fault condition of capacitor C132 is short-circuit;

– “Short_A_C135”, where the letter A applies to all components of the analog subsystem in cases where there is repetition of the reference designators in other subsystems (e.g. a C135 exists in the processor subsystem);
– ”Open_R34”, meaning that the fault condition of the resistor R34 is open-circuit;
– “Low_Output_U2”, meaning that the fault condition of the integrated circuit is low output.

A supplementary set of more specialized labels or names of events may be developed when required. However, it is important for the analyst to define and report those labels and names being used and ensure uniform and consistent use throughout a given fault tree analysis. This is particularly true if computer-aided techniques are to be used.

Consistency in labelling is even more important when a fault tree analysis software allows import of values for probability of occurrence of basic or primary events which are calculated in a spreadsheet based on bill of materials, components, components failure modes and their use profile. This may be the case when analysis is undertaken on a complex system. In this case, the labels – names for the basic and primary events – must be identical in both files (the spreadsheet and the fault tree analysis) so that the name matching allows import of probability of occurrence values to the corresponding events.

9 Report

The report of the fault tree analysis should include as a minimum the basic items listed below. Additional and supplementary information may be provided to increase clarity, especially in cases of complex systems analyses. A prescribed format is not proposed by this standard.

Basic items in the report should be as follows:

– objective and scope;
– system description: design description, system operation, detailed system boundaries definitions;
– assumptions: system design assumptions;
– operation, maintenance, test and inspection assumptions, reliability and availability modelling assumptions;
– analysing person/team with background and relevant expertise stated in the heading or in a separate section of the report: top event definition and criteria;
– references for basic events, undeveloped events and events analysed elsewhere, e.g. in different projects and justification for use of their probabilities (e.g., same stresses, same use profile, etc.);
– fault tree analysis: analysis, data, symbols used, common cause failures, where appropriate, minimal cut sets, where appropriate;
– results, conclusions, and recommendations.

Supplementary data items which may be included consist of

– system block or circuit diagrams;
– summary of reliability and maintainability data and sources used such as databases, information from the component manufacturers, filed information, etc.;
– FMEA/FMECA analysis or reference to the analysis.

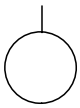
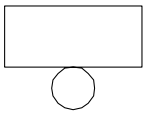
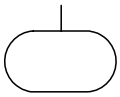
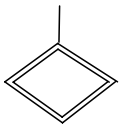
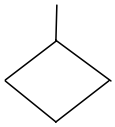
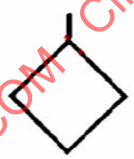
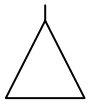
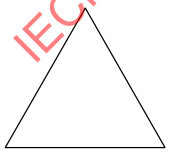
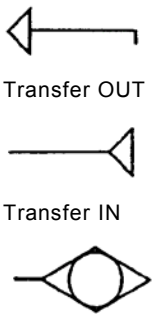
The FMEA table may be a useful method for representation of a concern, suggestions for design improvements, suggestions for verification of a concern, such as a test, and for the follow-up on those activities.

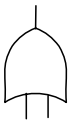
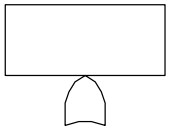
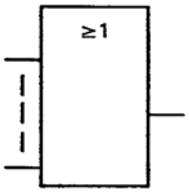
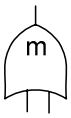
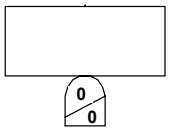
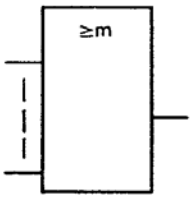
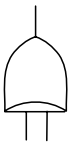
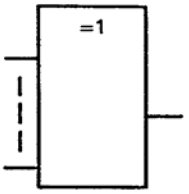
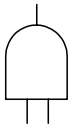
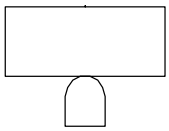
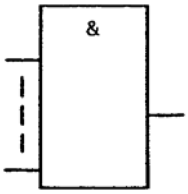
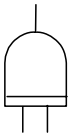
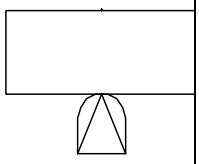
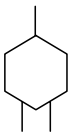
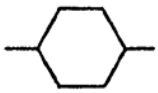
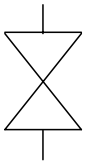
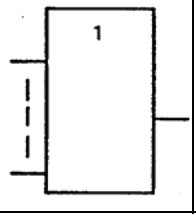
Annex A
(informative)

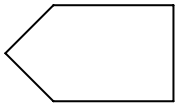
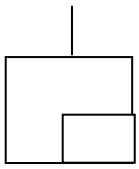
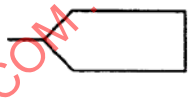
Symbols

The symbols shown in Table A.1 are commonly used.

Table A.1 – Frequently used symbols for a fault tree

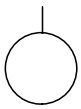
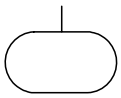
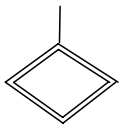
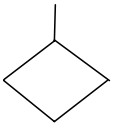
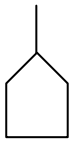
	Symbols		Name	Description	Reliability correlation	Number of inputs
			BASIC EVENT	The lowest level event for which probability of occurrence or reliability information is available	Component failure mode, or a failure mode cause	0
	—		CONDITIONAL EVENT	Event that is a condition of occurrence of another event when both have to occur for the output to occur	Occurrence of event that has to occur for another event to occur Conditional probability	0
			DORMANT EVENT	A primary event that represents a dormant failure; an event that is not immediately detected but could, perhaps, be detected by additional inspection or analysis	Dormant component failure mode or dormant failure cause	0
			UNDEVELOPED EVENT	A primary event that represents a part of the system that is not yet developed	A contributor to the probability of failure. Structure of that system part is not yet defined	0
			TRANSFER gate	Gate indicating that this part of the system is developed in another part or page of the diagram	A partial fault tree diagram that is shown in other location of the overall system IN means that the develop gate is elsewhere, OUT means that the same gate developed in this place will be used elsewhere	0

	Symbols		Name	Description	Reliability correlation	Number of inputs
			OR gate	The output event occurs if any of the input events occur	Failure occurs if any of the parts of that system fails – series system	≥ 2
			MAJORITY VOTE GATE	The output occurs if *m* or more inputs out of a total of *n* inputs occur	Redundancy k out of n, where $m = n - k + 1$	≥ 3
			EXCLUSIVE OR gate	The output event occurs if one, but not the other inputs occur	A failure of the system occurring only if one, not both of the two possible failures happens	≥2
			AND gate	The output event occurs only if all of the input events occur	Parallel redundancy, one out of n equal or different branches	≥ 2
			PRIORITY AND (PAND) gate	The output event (failure) occurs only if the input events occur in sequence from left to right	Good for representation of secondary failures or for enabling sequence of events	≥2; 2 (see comment on the SEQ gate)
			INHIBIT gate	The output occurs only if both of the input events take place, one of them conditional	Conditional probability of occurrence of the final event	2
			NOT gate	The output event occurs only if the input event does not occur	Exclusive events or preventive measure does not take place	1

	Symbols		Name	Description	Reliability correlation	Number of inputs
	 (This symbol was not a part of the group of previously standard symbols. It is a relatively new graphical representation of this gate)		SEQ (Sequential) gate	The output event (failure) occurs only if all input events occur in sequence from left to right. This gate is identical to the PAND gate if the number of inputs to the PAND gate is not limited to 2 as done by some analysts	Good for representation of sequential failures (chain failures). Also the sequence of stresses that would cause an event or a failure to occur. Requires Markov analysis	> 2
			SPARE gate	The output event will occur if the number of spare components is less than the number required	Representation of cold, warm and hot spare components. If all have exponential distribution, then the closed form solution exists. If probability of occurrence is constant, then Markov analysis is required. Other distributions may require conditional probabilities or simulations	≥ 1
			House event	Event which has happened, or will happen with certainty		
			Zero event	Event which cannot happen		

The above Table A.1 is not all inclusive. Some of the graphical gates or event representations that do not have comparison to other graphical representations are omitted from this table, but can be found in Tables A.2, A.3, and A.4.

Table A.2 – Common symbols for events and event description

Symbol	Symbol name	Definition	Description
	Basic event	The lowest level event for which probability of occurrence or reliability information is available	Failure mode of a component or an individual failure cause
	Conditional event	Event that is a condition of occurrence of another event when both have to occur for the output to occur	Conditional event required for output event to occur. It is used with PRIORITY AND and INHIBIT gates
	Dormant event	A primary event that represents a dormant failure; an event that is not immediately detected but could, perhaps, be detected by additional inspection or analysis	A primary event that might be detected by inspection, analysis or test
	Undeveloped event	A primary event that represents a part of the system that is not yet developed	A potential contributor to the occurrence of the top event, but relevant information for developing the event is currently unavailable
	House event	An event that is TRUE (turned ON) or FALSE (turned OFF). Can be a part of a fault tree that is included or excluded from analysis (ON or OFF)	A user-controlled event that allows analysis under alternate, defined system conditions

Static gates such as OR, AND, EXCLUSIVE OR, INHIBIT GATE and MAJORITY VOTE gates are shown in Table A.3.

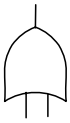
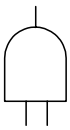
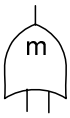
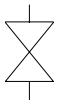
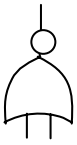
The dynamic gates such as PRIORITY AND gate, SEQUENTIAL gate and SPARE gate, are shown in Table A.4.

Example of the dynamic PRIORITY AND gate:

Description of events:

Diode D1 protects the IC from over-current due to the supply voltage surge. The IC does not get damaged by the voltage surge if diode does not fail first in the open mode. If the diode opens, and the second event takes place, whilst there exists a voltage surge, then the top event (IC explodes) takes place. The model is shown in Figure A.1.

Table A.3 – Static gates

Gate name	Description	Reliability model	Number of inputs
OR gate 	The output event occurs if any of the input events occur	Series events, when independent: i = 2 to n $F(t) = 1 - \prod_{i=2}^{n} [1 - F_i(t)]$ (where events are not independent, see [disjointing], 7.5.5.4), $F(t)$ – probability of event occurrence or fault existence at time t. $R(t)$, when used, is a complement of the $F(t)$	≥2
AND gate 	The output event occurs only if all of the input events occur	Parallel redundancy, equal or different independent branches $F(t) = \prod_{i=2}^{n} F_i(t)$ (where events are not independent, see [disjointing] 7.5.5.4)	≥2
MAJORITY VOTE gate 	The output event occurs if m or more inputs out of a total of n inputs occur	Parallel redundancy where k out of n the branches is not failed $m = n - k + 1$ When all inputs equal: $F(t) = \sum_{i=0}^{k-1} \frac{n!}{i!(n-i)!} \cdot [1 - F_0(t)]^i \cdot [F_0(t)]^{n-i}$ (where events are not independent, see [disjointing], 7.5.5.4)	≥2
NOT Gate 	The output event occurs only if the input event does not occur	$F(t) = 1\text{-}F_1(t)$ NOTE It is advised that this gate be used carefully by an experienced analyst to avoid unwanted results.	1
Exclusive OR (XOR) gate 	The output event occurs if one, but not the other inputs occur	A top event occurs only if one, but not the other event occur $F(t) = F_1(t) \cdot [1 - F_2(t)]$	=2
NOR gate 	The output occurs if none of the input events occur	It acts as a combination of NOT and OR gate. The output is FALSE if there is one or more TRUE inputs $F(t) = \prod_{i=2}^{n} [1 - F_i(t)]$ NOTE It is advised that this gate be used carefully by an experienced analyst to avoid unwanted results.	≥2

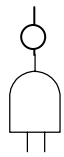
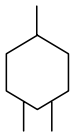
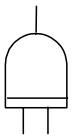
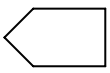
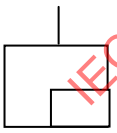
Gate name	Description	Reliability model	Number of inputs
NAND gate 	The output occurs if at least one of the input events does not	The gate functions as a combination of NOT and AND gates $F(t) = \prod_{i=1}^{k}[1 - F_i(t)] \cdot \prod_{ij=k}^{n-k}[F_j(t)]$ NOTE It is advised that this gate be used carefully by an experienced analyst to avoid unwanted results.	≥2
INHIBIT gate 	The output occurs only if both of the input events take place one of them conditional	The probability of occurrence is the probability of occurrence of input event multiplied by the probability of occurrence of the condition being satisfied	2

Table A.4 – Dynamic gates

Gate name	Description	Comment	Number of inputs
Priority AND gate (PAND) 	The output event (failure) occurs only if all input events occur in sequence from left to right	Good for representation of secondary failures or for enabling sequence of two or more events. If more than two events, it is equal to the SEQUENCE ENFORCING gate. Requires Markov analysis	≥2 (see SEQ gate below)
Sequential gate, SEQ 	The output event occurs only if all input events occur in sequence from left to right, and there are more than two input events. This gate is an alternative to the PAND gate above	This gate is an extension of PAND gate and as such included to emphasize the sequence of many gates. In that case, its original gate, PAND, is limited to two inputs only. Good for representation of sequential failures (chain failures). Also the sequence of stresses that would cause an event or a failure to occur requires Markov analysis	>2
Spare gate; SPARE 	The output event will occur if the number of spare (standby redundant) components is less than the number required	Representation of cold, warm and hot spare components. If all have exponential distributions, then the closed form solution may exist. If probability of occurrence of input events is constant, then Markov analysis is required. Other distributions may require conditional probabilities or simulations. Spare components have reduced probability of failure before during the time they are not activated (see 7.5.3 for cold and warm redundancy modelling)	≥1

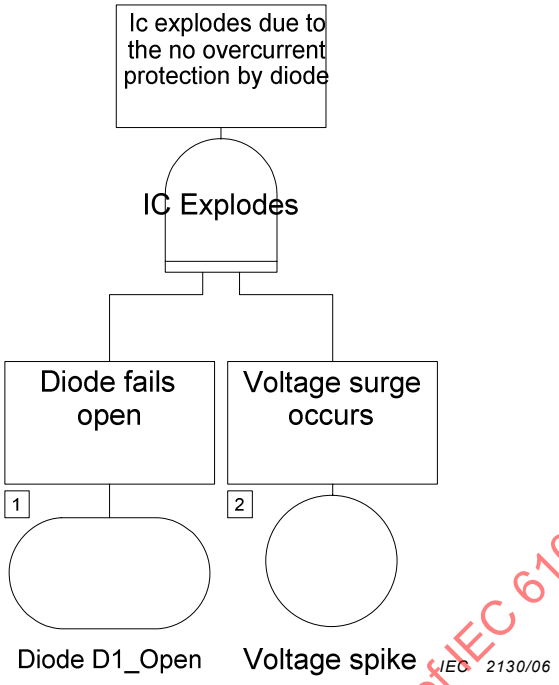


Figure A.1 – Example of a PAND gate

Annex B
(informative)

Detailed procedure for disjointing

B.1 Success approach

Suppose the reliability block diagram represents a network consisting of five elements A, B, C, D and E and that a, b, c, d and e denote the corresponding Boolean "success" variables. It is also supposed that system success (SS) in Boolean terms is defined by the following expression, which comprises four sum-of-product terms:

$$SS = ac + bd + aed + bec$$

To make the above expression disjoint, the procedure is as follows:

Step 1.1: Make each term disjoint with respect to the first. Proceed in a systematic way to make the second term disjoint with respect to the first. Inspect the two terms to see if any variable in the first appears in complemented form in the second. If this is so, the two terms are already disjoint and there is nothing further to do. If not, pick out all the variables in the first term (***ac***), which do not appear in the second (bd). (In set theory terminology this is called the relative complement of the second term with respect to the first). In this particular step the result is the variables a and c.

Step 1.2: Replace the second term bd by $\bar{a}bd + a\bar{c}bd$.

Step 1.3: Make the third term disjoint with respect to the first. First of all, inspect the two terms to see if any variable in the first appears in complemented form in the second. Since this is not so, identify the relative complement of the third term with respect to the first: namely the variable c. Hence replace the third term by the term $\bar{c}aed$.

Step 1.4: Make the fourth term (bec) disjoint with respect to the first. The relative complement of the fourth term with respect to the first is the variable a. Therefore replace the fourth term by $\bar{a}bec$. The system success expression at this stage thus becomes:

$$SS_1 = ac + \bar{a}bd + a\bar{c}bd + \bar{c}aed + \bar{a}bec$$

Now repeat the process starting with the second term.

Step 2.1: Make the third term of SS_1 ($a\bar{c}bd$) disjoint with respect to the second ($\bar{a}bd$). In this instance the terms are already disjoint (on account of variable a), so there is nothing further to do.

Step 2.2: Make the fourth term of SS_1 ($\bar{c}aed$) disjoint with respect to the second ($\bar{a}bd$). In this instance also, note the terms are already disjoint (on account of variable a) so there is nothing further to do.

Step 2.3: Make the fifth term of SS_1 ($\bar{a}bec$) disjoint with respect to the second ($\bar{a}bd$). The relative complement is the variable d so replace the fifth term by $\bar{d}\bar{a}bec$.

The system success expression at this stage thus becomes:

$$SS_2 = ac + \bar{a}bd + a\bar{c}bd + \bar{c}aed + \bar{d}\bar{a}bec$$

Now repeat the process starting with the third term.

Step 3.1: Make the fourth term of SS_2 $(\bar{c}aed)$ disjoint with respect to the third $(a\bar{c}bd)$. The relative complement is the variable b so replace the fourth term by $\bar{b}\bar{c}aed$.

Step 3.2: Make the fifth term of SS_2 $(\bar{d}\bar{a}bec)$ disjoint with respect to the third $(a\bar{c}bd)$. In this instance the terms are already disjoint (on account of variables a, c and d), so there is nothing further to do.

The system success expression at this stage is

$$SS_3 = ac + \bar{a}bd + a\bar{c}bd + \bar{b}\bar{c}aed + \bar{d}\bar{a}bec$$

and since no further simplification appears possible, this is the final disjointed expression.

Making the usual substitutions, the equation for system reliability is given by:

$$R_{S1} = R_aR_c + (1-R_a)R_bR_d + R_a(1-R_c)R_bR_d + (1-R_b)(1-R_c)R_aR_eR_d + (1-R_d)(1-R_a)R_bR_eR_c$$

It should be noted that the form of the final result, in this case SS_3, will depend on the order in which the terms in the original Boolean expression are written down.

By using the theorem of total probability, it can be shown that the expression for system reliability can be written in the form:

$$R_{S2} = (R_a + R_b - R_aR_b)(R_c + R_d - R_cR_d)R_e + (R_aR_c + R_bR_d - R_aR_cR_bR_d)(1-R_e)$$

Although the expressions for R_{S1} and R_{S2} look quite different, they are in fact identical.

B.2 System failure, SF, (cut sets) approach

Disjointing is explained as follows:

$$SF = ab + cd + aed + bec$$

To make the above expression disjoint, the procedure is as follows:

Step 1.1: Make each term disjoint with respect to the first. Proceed in a systematic way to make the second term disjoint with respect to the first. Inspect the two terms to see if any variable in the first appears in complemented form in the second. If this is so, the two terms are already disjoint and there is nothing further to do. If not, pick out all the variables in the first term (ab), which do not appear in the second (cd). (In set theory terminology this is called the relative complement of the second term with respect to the first.) In this particular step the result is the variables a and b.

Step 1.2: Replace the second term cd by $\bar{a}cd + a\bar{b}cd$.

Step 1.3: Make the third term disjoint with respect to the first. First of all, inspect the two terms to see if any variable in the first appears in complemented form in the second. Since this is not so, identify the relative complement of the third term with respect to the first: namely the variable b. Hence replace the third term by the term $\bar{b}aed$.

Step 1.4: Make the fourth term (***bac***) disjoint with respect to the first. The relative complement of the fourth term with respect to the first is the variable a. Therefore replace the fourth term by $\bar{a}bec$. The system failure expression at this stage thus becomes:

$$SF_1 = ab + \bar{a}cd + a\bar{b}cd + \bar{b}aed + \bar{a}bec$$

Now repeat the process starting with the second term. Hence:

Step 2.1: Make the third term of SF_1 $(a\bar{b}cd)$ disjoint with respect to the second $(\bar{a}cd)$. In this instance, the terms are already disjoint (on account of variable a), so there is nothing further to do.

Step 2.2: Make the fourth term of SF_1 $(\bar{b}aed)$ disjoint with respect to the second $(\bar{a}cd)$. In this instance also, note the terms are already disjoint (on account of variable a) so there is nothing further to do.

Step 2.3: Make the fifth term of SF_1 $(\bar{a}bec)$ disjoint with respect to the second $(\bar{a}cd)$. The relative complement is the variable d so replace the fifth term by $\bar{d}\bar{a}bec$.

The system failure expression at this stage thus becomes:

$$SF_2 = ab + \bar{a}cd + a\bar{b}cd + \bar{b}aed + \bar{d}\bar{a}bec$$

Now repeat the process starting with the third term. Hence:

Step 3.1: Make the fourth term of SF_2 $(\bar{b}aed)$ disjoint with respect to the third $(a\bar{b}cd)$. The relative complement is the variable c so replace the fourth term by $\bar{b}\bar{c}aed$.

Step 3.2 Make the fifth term of SF_2 $(\bar{d}\bar{a}bec)$ disjoint with respect to the third $(a\bar{b}cd)$. In this instance, the terms are already disjoint (on account of variables a and d, and according to the defined format), so there is nothing further to do.

The system failure expression at this stage is:

$$SF_3 = ab + \bar{a}cd + a\bar{b}cd + \bar{b}\bar{c}aed + \bar{d}\bar{a}bec$$

and since no further simplification appears possible, this is the final disjointed expression.

Making the usual substitutions, the equation for system failure is given by:

$$F_{S1} = F_a F_b + (1 - F_a) F_c F_d + F_a (1 - F_b) F_c F_d + (1 - F_b)(1 - F_c) F_a F_e F_d + (1 - F_d)(1 - F_a) F_b F_e F_c$$

It should be noted that the form of the final result, in this case SF_3, will depend on the order in which the terms in the original Boolean expression are written down.

Bibliography

[1] NASA Office of Safety and Mission Assurance: Fault Tree Handbook for Aerospace Applications, Version 1.1, 2002

[2] US Nuclear Regulatory Commission: NUREG 0492, fault Tree Handbook, January, 1981

[3] Mohame Modarres, Mark Kaminskiy, Vasiliy Krivitsov: Reliability Engineering and Risk Analysis, Marcel Dekker Inc.,new York, 1999

[4] Alfredo H-S. Ang, Wilson H. Tang: Probability Concepts in Engineering Planning and Design, 1990

[5] Milena Krasich: Fault Tree Analysis for Failure Mode Identification and Product Reliability Improvement, Tutorial, RAMS, 2005, Alexandria, VA

[6] Systems" 1999 Tutorial Notes, Reliability and Maintainability Symposium, Washington, DC

[7] Kiran Kumar Vemuri and Joanne Bechta Dugan, "Reliability Analysis of Complex Hardware-Software Systems", Proceedings, Annual Reliability and Maintainability Symposium, January 1999, Washington, DC

[8] Géza Szabó and Péter Gáspár, "Practical Treatment Methods for Adaptive Components in the Fault-Tree Analysis", Proceedings, Annual Reliability and Maintainability Symposium, January 1999, Washington, DC

[9] IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

[10] IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

[11] IEC 61078, A*nalysis techniques for dependability – Reliability block diagram and boolean methods*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ANALYSE PAR ARBRE DE PANNE (AAP)

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61025 a été préparée par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
56/1142/FDIS	56/1162/FDIS

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette deuxième édition annule et remplace la première édition publiée en 1990. Elle constitue une révision technique.

Les principaux changements par rapport à l'édition précédente sont les suivants:

– ajout d'explications détaillées sur les méthodologies de l'arbre de panne
– ajout d'aspects quantitatifs et d'aspects de fiabilité sur l'Analyse par Arbre de Panne (AAP)
– extension de la relation avec d'autres techniques de sûreté de fonctionnement
– ajout d'exemples d'analyses et de méthodes expliqués dans cette norme
– mise à jour des symboles couramment utilisés

L'Article 7 concernant les analyses a été modifié afin de traiter l'analyse par arbre de panne logique traditionnelle séparément de l'analyse quantitative utilisée depuis de nombreuses années, pour l'amélioration de la fiabilité des produits pendant leur développement.

Certaines parties intégrées précédemment dans le corps de cette norme, ont été transférées aux Annexes A et B.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

L'AAP sert à déterminer et à analyser les conditions et les facteurs qui produisent, peuvent potentiellement produire ou contribuent à produire un événement indésirable défini. Pour l'AAP, cet événement est généralement un «grippage» ou une dégradation des performances du système, de la sécurité ou d'autres attributs fonctionnels importants, alors qu'avec l'analyse par arbre de succès (STA = Success Tree Analysis) cet événement est l'attribut décrivant le succès.

L'AAP est souvent appliquée aux analyses pour la sécurité des systèmes (tels que les systèmes de transport, les centrales électriques, ou tout autre système pouvant nécessiter une évaluation de la sécurité de leur fonctionnement). L'analyse par arbre de panne peut également être utilisée pour les analyses de disponibilité et de maintenabilité. Cependant, dans le reste de cette norme, à fin de simplification, le terme de fiabilité sera utilisé pour représenter ces aspects de performance du système.

Dans cette norme, deux approches de l'AAP sont traitées. L'une d'elles est une approche qualitative, où la probabilité des événements et leurs facteurs de contribution – les événements d'entrée ou leur fréquence d'apparition n'est pas traitée. Cette approche est une analyse détaillée des événements/pannes et est connue comme AAP Qualitative ou traditionnelle. Elle est largement utilisée dans les applications de l'industrie nucléaire et de nombreuses autres instances où les causes potentielles, – les pannes sont recherchées quelque soit leur fréquence d'apparition. Parfois, certains événements dans l'analyse traditionnelle sont étudier quantitativement, mais ces calculs sont dissociés de tout autre concept de fiabilité d'ensemble, auquel cas, aucune tentative pour calculer la fiabilité d'ensemble en utilisant l'AAP n'est faite. La seconde approche adoptée par de nombreuses industries est largement quantitative, dans les cas d'AAP qui modélisent un produit complet, un procédé, ou un système et la grande majorité d'événements de base, pannes ou événements, qui a une probabilité d'apparition déterminée par analyse ou essai. Dans ce cas, le résultat final est la probabilité d'apparition d'un événement de tête représentant la fiabilité ou la probabilité d'une panne ou d'une défaillance.

ANALYSE PAR ARBRE DE PANNE (AAP)

1 Domaine d'application

La présente Norme internationale décrit l'analyse par arbre de panne et donne des lignes directrices sur son application comme suit:

– définition des principes de base;
  - en définissant et en expliquant la modélisation mathématique associée;
  - en expliquant les relations entre l'AAP et d'autres techniques de modèle de fiabilité;
– description des étapes impliquées dans la réalisation de l'AAP;
– identification des hypothèses appropriées, des événements et des modes de défaillance;
– identification et description des symboles couramment utilisés.

2 Références normatives

Les documents référencés suivants sont indispensables pour l'application de ce document. Pour des références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition du document référencé (y compris les amendements) qui s'applique.

CEI 60050(191), *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service.*

CEI 61165, *Application des techniques de Markov*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60050(191) s'appliquent.

Dans la méthodologie et les applications de l'arbre de panne, de nombreux termes sont utilisés pour mieux expliquer l'objectif de l'analyse ou le mécanisme de pensée que reflète une telle analyse. Il s'agit de termes utilisés également comme synonymes de ceux qui sont considérés comme analytiquement corrects par divers auteurs. Les termes supplémentaires suivants sont utilisés dans la présente norme.

3.1
issue
résultat d'une action ou autre entrée; conséquence d'une cause

NOTE 1 Une issue peut être un événement ou un état. Dans un arbre de panne, une issue d'une combinaison d'événements d'entrée correspondants représentés par une porte peut être soit un événement intermédiaire ou un événement de tête.

NOTE 2 Dans un arbre de panne, une issue peut également être une entrée vers un événement intermédiaire ou elle peut être un événement de tête.

3.2
événement de tête
issue de combinaisons de tout événement d'entrée

NOTE 1 C'est l'événement intéressant sous lequel un arbre de panne est développé. On fait souvent référence à l'événement de tête par l'**événement final**, ou l'**issue de tête**.

NOTE 2 L'événement de tête est prédéfini et est le point de départ d'un arbre de panne. Il a une position supérieure dans la hiérarchie des événements.

3.3
événement final
résultat final de combinaisons de tous les événements d'entrée intermédiaires et de base

NOTE Il s'agit d'un résultat d'événements d'entrée ou d'états (voir 3.2).

3.4
issue de tête
issue qui est étudiée en construisant l'arbre de panne

NOTE Résultat final de combinaisons de tous les événements d'entrée intermédiaire et de base, c'est un résultat d'événements d'entrée ou d'états (voir 3.2).

3.5
porte
symbole qui est utilisé pour établir un lien symbolique entre l'événement de sortie et les entrées correspondantes

NOTE Un symbole de porte donné réfléchit le type de relation nécessaire entre les événements d'entrée pour qu'un événement de sortie apparaisse.

3.6
coupe
groupe d'issues (ou d'événements) qui, si tous se produisent, provoquerait l'apparition de l'événement de tête

3.7
coupe minimale
minimum, ou plus petit ensemble d'événements devant se produire pour causer l'événement de tête

NOTE La non-apparition de l'un ou l'autre des événements de l'ensemble empêcherait l'apparition de l'événement de tête.

3.8
événement
apparition d'une condition ou d'une action

3.9
événement de base
événement ou état qui ne peut pas être développé plus

3.10
événement primaire
événement qui se situe en bas de l'arbre de panne

NOTE Dans la présente norme, un événement primaire peut signifier un événement de base qui ne peut plus être développé ou il peut s'agir d'un événement qui, bien qu'il soit un produit de groupes d'événements et de portes, peut être développé ailleurs ou ne pas être développé du tout (événement non développé).

3.11
événement intermédiaire
événement qui est ni un événement de tête ni un événement primaire

NOTE Il est généralement le résultat d'un ou de plusieurs événements primaires et/ou d'autres événements intermédiaires.

3.12
événement non développé
événement qui n'a aucun événement d'entrée

NOTE Dans l'analyse, il n'est pas développé pour diverses raisons possibles, tel que le manque d'information plus détaillée, ou il est développé dans une autre analyse et ensuite annoté dans l'analyse en cours comme non développé. Un des exemples de portes non développées serait Commercial Of The Shelf items ou COTS

3.13
défaillance localisée (événement)
défaillance qui, si elle apparaît, causerait la défaillance du système global ou serait en elle-même la cause de l'événement de tête non favorable (issue) indépendamment des autres événements ou de leurs combinaisons

3.14
événements de cause commune
différents événements dans un système ou un arbre de panne qui ont la même cause d'apparition

NOTE Un exemple d'un tel événement serait la réduction de condensateurs céramique due à la flexion de carte imprimée; par conséquent même si ceux-ci sont des condensateurs différents avec des fonctions différentes dans la conception, leur réduction causerait la même chose – le même événement d'entrée.

3.15
cause commune
cause d'apparition d'événements multiples

NOTE Dans l'exemple ci-dessus, la flexion de la carte serait l'événement intermédiaire qui lui-même résulte de multiples événements tels que: choc environnemental, vibrations ou rupture manuelle de carte imprimée pendant la fabrication du produit.

3.16
événement répliqué ou répété
événement qui est une entrée à plus d'un événement de niveau supérieur

NOTE Cet événement peut être une cause commune ou un mode de défaillance d'un composant partagé par plus d'une partie de la conception.

La Figure 1 illustre les définitions ci-dessus. Cette figure contient les annotations et descriptions d'événements pour mieux expliquer l'application pratique d'un arbre de panne. Les explications graphiques des coupes ou coupes minimales sont omises de la Figure 1, pour simplifier la représentation graphique d'autres termes pertinents. Les symboles dans la Figure 1 et toutes les figures suivantes semblent quelque peu différents de ceux des Tableaux A.1, A.2, A.3 et A.4 à cause de la boîte ajoutée au-dessus du symbole de la porte pour la description des événements individuels.

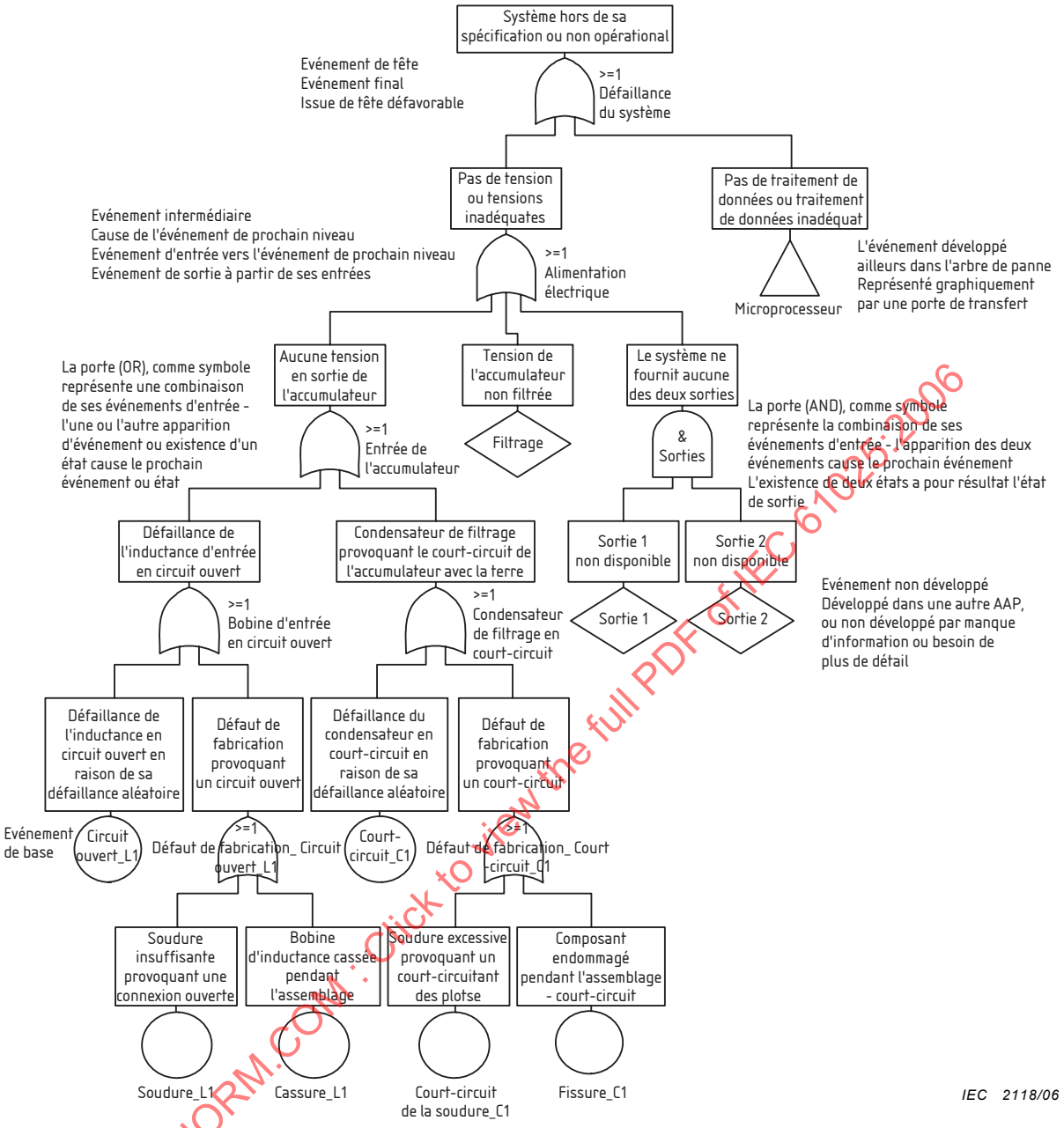


Figure 1 – Explication des définitions utilisées dans les analyses par arbre de panne

NOTE Les symboles dans la Figure 1 et dans toutes les autres figures peuvent être sensiblement différents des symboles présentés dans l'Annexe A. Ceci est dû aux blocs de description ajoutés pour une meilleure explication de la relation entre les différents événements.

4 Symboles

La représentation graphique d'un arbre de panne requiert l'utilisation d'un ensemble cohérent de symboles, de repères et de libellés. Les symboles varient avec les préférences des utilisateurs et les progiciels éventuellement utilisés. Un guide général est donné à l'Article 8 et à l'Annexe A.

D'autres symboles utilisés dans cette norme sont des symboles de sûreté de fonctionnement normalisés tels que $F(t)$ ou juste la probabilité d'apparition d'un événement F. Pour cette raison, une liste séparée des symboles n'est pas fournie.

5 Généralités

5.1 Structure et description de l'arbre de panne

L'analyse par arbre de panne (AAP) est une méthode parmi d'autres d'analyse de la sûreté de fonctionnement. Avant de commencer une AAP, Il convient que l'analyste examine l'objectif de chaque méthode et son applicabilité individuelle ou combinée dans l'évaluation du flux d'événements ou d'états qui seraient la cause d'une issue, ou la fiabilité ou disponibilité d'un système donné ou de composant. Il convient de tenir compte des avantages et des inconvénients de chaque méthode et de leurs produits respectifs, des données nécessaires pour effectuer l'analyse, de la complexité de l'analyse, ainsi que d'autres facteurs identifiés dans la présente norme.

Un arbre de panne constitue une représentation graphique organisée des conditions ou des facteurs produisant ou contribuant à produire un événement indésirable défini, appelé «événement de tête». Lorsque l'issue est un succès, alors l'arbre de panne devient un arbre de succès, ou les événements d'entrée sont ceux qui contribuent à l'événement de succès de tête. Cette représentation est établie sous une forme clairement compréhensible, analysable et, si nécessaire, adaptable pour faciliter l'identification:

– des facteurs influant sur l'événement de tête à l'étude comme dans la plupart des analyses d'arbre de panne traditionnelles;
– des facteurs influant sur la fiabilité et sur les caractéristiques fonctionnelles du système, lorsque la technique AAP est utilisée par l'analyse de la fiabilité, par exemple imperfections de conception, contraintes environnementales ou de fonctionnement, modes de défaillance des composants, erreurs de l'opérateur, erreurs dans le logiciel;
– des événements influant sur plus d'un composant fonctionnel et qui pourraient annuler le bénéfice apporté par les redondances spécifiques ou influer sur deux ou plusieurs parties d'un produit, qui peuvent autrement sembler non liées d'un point de vue opérationnel ou indépendants (événements de cause commune).

L'analyse par arbre de panne est une méthode d'analyse déductive (descendante) qui a pour but de faire apparaître les causes ou les combinaisons de causes qui peuvent produire l'événement de tête défini. Cette analyse peut être qualitative ou quantitative, en fonction de la portée des analyses.

Un arbre de panne peut être développé comme son complément, le Success Tree Analysis (STA) Analyse de l'Arbre de Succès, lorsque l'événement de tête est un succès, et ses entrées ont contribué au succès (souhaité).

Dans les cas où la probabilité d'apparition des événements primaires ne peut pas être estimée, une AAP qualitative peut être utilisée pour rechercher les causes d'issues défavorables potentielles avec des événements primaires individuels et portant une indication descriptive de la probabilité d'apparition telle que: «fortement probable», «très probable», «probabilité moyenne», «probabilité éloignée», etc. Le premier but d'une AAP qualitative est d'identifier la coupe minimale afin de déterminer les manières dont les événements primaires ou de base influencent l'événement de tête.

Une AAP quantitative peut être utilisée, lorsque les probabilités d'événements de base sont connues. Les probabilités d'apparition de tous les événements intermédiaires et de l'événement de tête (issue) peuvent ensuite être calculées. L'AAP quantitative est également très utile dans l'analyse de fiabilité d'un produit ou d'un système dans son développement.

L'AAP peut être utilisée pour l'analyse des systèmes ayant des interactions complexes entre les sous-systèmes, interactions logicielles/matérielles incluses.

5.2 Objectifs

L'AAP peut être entreprise seule ou combinée à d'autres analyses de fiabilité. Les objectifs sont les suivants:

– identifier les causes ou les combinaisons de causes conduisant à l'événement de tête;

– déterminer si l'une des caractéristiques de fiabilité du système est conforme à une exigence établie;

– déterminer quel(s) mode(s) ou facteur(s) de défaillance potentiel(s) contribuerai(en)t le plus à la probabilité, pour le système, de défaillance (fiabilité insuffisante) ou d'impossibilité, lorsqu'un système est réparable, d'améliorations de la fiabilité du système;

– analyser et comparer les diverses alternatives de conception, afin d'améliorer la fiabilité du système;

– démontrer que les hypothèses faites dans d'autres analyses (telles que Markov et FMEA) sont valables;

– identifier les modes de défaillance potentiels qui pourraient être à l'origine d'un problème de sécurité, évaluer la probabilité d'apparition correspondante et la possibilité de réduction;

– Identifier les événements communs (par exemple, la branche moyenne d'un circuit à embranchement, voir Figure 10);

– rechercher un événement ou des combinaisons d'événements qui sont le plus susceptibles de provoquer l'apparition de l'événement de tête;

– évaluer l'impact (l'importance) de l'apparition d'un événement primaire sur la probabilité de l'événement de tête;

– calculer les probabilités d'événement;

– calculer les taux de disponibilité et de défaillance du système ou de ses composants représentés par un arbre de panne, évaluer si des conditions continues peuvent être établies et si les réparations éventuelles sont indépendantes les unes des autres (même limitation que pour le diagramme du cheminement pour le succès/bloc-diagramme de fiabilité).

5.3 Applications

L'AAP est particulièrement adaptée à l'analyse de systèmes constitués de plusieurs sous-systèmes dépendants ou entre lesquels existent des relations fonctionnelles. Les avantages de l'AAP sont clairs dans le cas d'une conception d'un système qui est le produit de plusieurs groupes de conception technique spécialisés indépendants et lorsque les AAP partielles sont reliées. L'analyse par arbre de panne est couramment appliquée lors de la conception des centrales nucléaires, des systèmes de transport, des systèmes de communication, des procédés chimiques et autres procédés industriels, des réseaux ferroviaires, des matériel hifi et vidéo, des systèmes médicaux, des systèmes informatiques, etc. L'analyse par arbre de panne présente également un intérêt particulier lorsqu'elle s'applique à des systèmes comprenant des composants de natures diverses et à leurs interactions (composants mécaniques, électroniques et logiciels) qui ne peuvent être modélisés par d'autres techniques. Un exemple de ceci serait une combinaison d'événements où l'ordre d'apparition est essentiel tel que l'existence de fatigue due aux vibrations provoquant des fissures et des défaillances de composants.

L'AAP possède une multitude d'utilisation comme outil (pour en citer quelques-unes):

– déterminer la combinaison logique pertinente d'événements menant à l'événement de tête et leur mise en priorité potentielle ;

– étudier un système en développement et anticiper ou prévenir et atténuer les causes potentielles d'un événement de tête non souhaité ;

– analyser un système, déterminer sa fiabilité, identifier les éléments principaux contribuant à sa fiabilité et évaluer les modifications de conception ;

– aider aux efforts d'évaluation du risque de probabilité.

L'AAP peut être appliquée à tous les produits nouveaux ou modifiés dans toutes les phases de conception, comme un outil analytique pour l'identification des problèmes potentiels de conception, y compris dans les premières phases pour lesquelles les informations de détail sur la conception sont incomplètes. Ces efforts anticipés peuvent être ensuite poursuivis, lorsque davantage d'informations sur la conception du système et sur ses composants deviennent disponibles. L'AAP traite également de problèmes potentiels qui peuvent provenir de la conception physique du produit, de contraintes environnementales ou de fonctionnement, de failles dans les processus de fabrication du produit, et de procédures de fonctionnement et de maintenance.

5.4 Combinaisons avec d'autres techniques d'analyse de fiabilité

5.4.1 Combinaison de l'AAP avec l'analyse des modes de défaillance et de leurs effets (AMDE)

Cette combinaison d'analyses est souvent recommandée par des normes spécifiques sectorielles, en particulier des normes de sécurité et des normes sur les modes de transport. Les bénéfices d'une analyse combinée sont les suivants:

– l'AAP est une méthode d'analyse descendante et l'AMDE est une méthode d'analyse ascendante, et une confrontation des raisonnements déductif et inductif est considérée comme un bon argument pour assurer l'intégralité d'une analyse ;

– les normes de sécurité exigent souvent une analyse des défaillances individuelles et une analyse des défaillances multiples, la première exigence étant satisfaite par l'AMDE. Les analyses des défaillances individuelles et multiples sont accomplies par l'AAP ;

– l'AMDE est également une méthode utile pour une identification détaillée des événements de base ou des risques, tandis que l'AAP est une méthode pratique d'analyse causale des événements indésirables.

De plus, il existe un contrôle de cohérence simple entre l'AMDE et l'AAP :

– toute défaillance individuelle identifiée dans l'AMDE conduisant à un événement de tête de l'arbre de panne doit également apparaître en tant que défaillance localisée (dans la coupe minimale);

NOTE Une défaillance localisée est une défaillance qui, si elle se produit, entraîne la défaillance de l'ensemble du système.

– il convient que toute défaillance localisée identifiée dans l'AAP apparaisse en tant que telle dans l'AMDE.

La valeur de ce contrôle de cohérence est accrue si les analyses sont réalisées séparément et indépendamment. Cela est particulièrement important dans les analyses de sécurité.

La norme CEI qui explique cette méthodologie est la CEI 60300-3-1.

5.4.2 Combinaison de l'AAP avec l'analyse par arbre d'événement (AAE)

Tout événement indésirable pourrait être analysé par l'AAP. Cependant, dans certains cas, cela peut ne pas être approprié, pour plusieurs raisons:

– il est parfois plus simple d'élaborer des séquences d'événements plutôt que des relations causales;

– les arbres résultants peuvent devenir très ramifiés;

– ce sont souvent des équipes indépendantes qui dirigent les différentes parties de l'analyse.

Pour trouver une procédure pratique, souvent ce n'est pas de l'événement de tête non désiré qui est défini en premier, mais des événements potentiellement indésirables à l'interface entre le domaine opérationnel et le domaine technique.

A titre d'illustration, considérons pour une mission spatiale, l'événement de tête non désiré «perte de l'équipage ou du véhicule spatial». Au lieu de construire un grand arbre de panne basé sur la «perte de l'équipage ou de véhicule spatial», des événements intermédiaires non désirés tels que «panne d'allumage» ou «défaillance moteur» peuvent être définis comme des événements de tête et analysés comme des arbres de panne séparés. Ces événements de tête réduits pourront être ensuite utilisés comme des entrées vers un arbre d'événement, afin d'analyser les conséquences opérationnelles.

Cette combinaison de l'AAE et de l'AAP est parfois désignée sous le terme d'analyse de cause à effet (ACE).

5.4.3 Combinaison de l'AAP avec l'analyse de Markov

Une AAP qui est seulement une combinaison d'événements statiques (le délai – la séquence de la combinaison d'événement n'est pas considérée ou modélisée – portes statiques) évalue généralement les systèmes hors de la dépendance de la séquence des événements. Cependant, il est possible d'étendre l'AAP statique en définissant des portes supplémentaires qui représentent les modèles de Markov. Ces portes portent le nom de portes «dynamiques» et comprennent des portes PRIORITY AND, SEQUENTIAL et SPARE. Pour de telles portes, il est nécessaire d'évaluer la probabilité de défaillance à un temps t en utilisant le modèle ou la simulation de Markov approprié(e). Une fois évaluée, la porte dynamique et ses entrées peuvent être remplacées par un événement primaire simple, avec la probabilité d'apparition calculée par l'analyse de Markov. Certains logiciels du commerce permettent la modélisation de portes dynamiques et offrent la capacité de calcul de probabilité d'apparition de l'événement représenté par la porte. Un exemple de porte dynamique PRIORITY AND est présenté à l'Annexe A.

Les portes statiques et dynamiques d'un arbre de panne sont utilisées en se basant sur l'hypothèse que les événements individuels sont indépendants (sauf s'ils sont définis comme communs). Cependant, une attention particulière doit être accordée aux propriétés d'indépendance entre les événements dans le modèle de Markov et les événements dans l'arbre de panne.

5.4.4 Combinaison des techniques de l'AAP et du diagramme de décision binaire (DDB)

Le calcul de la probabilité d'apparition pour un événement de tête d'un arbre de panne avec de nombreuses coupes nécessite les calculs de probabilité pour toutes les combinaisons de coupes. A cause de sa haute complexité, ce calcul sera souvent tronqué. Un diagramme de décision binaire (DDB) peut être construit de façon récursive à partir d'un arbre de panne et peut fournir une méthode de calcul efficace et exacte. Cette méthode est bien expliquée dans le «NASA Fault Tree Handbook with Aerospace Applications version 1.1[1][1]».

L'approche du DDB est utile lorsque la troncature des calculs de la probabilité de coupe entraîne une perte inacceptable de précision ou si la solution AAP prend trop de temps, en particulier lorsque de nombreux événements de forte probabilité apparaissent dans le modèle. En raison de la disjonction des cheminements minimaux générés dans l'approche du DDB, (voir 7.5.5.4), le calcul de l'importance et des sensibilités peut également être réalisé efficacement et avec exactitude.

[1] Les chiffres entre crochets se réfèrent à la bibliographie.

5.4.5 Combinaison avec le bloc-diagramme de fiabilité

Un bloc-diagramme de fiabilité est constitué de blocs ou modules, représentant un groupe de composants, ou de modes de défaillance. Ces groupes sont normalement formés suivant le bloc-diagramme fonctionnel d'un produit, système, ou procédé. Ces modules ont soit un taux de défaillance déterminé, soit une fiabilité calculée ou une probabilité de défaillance pour une utilisation donnée ou un profil opérationnel. Traditionnellement, il convient que les blocs aient un taux de défaillance équivalent à la somme des taux de défaillance des composants individuels. De cette manière, l'interaction fonctionnelle des composants dans un module n'est pas considérée.

Pour augmenter l'exactitude de la modélisation fonctionnelle dans un bloc (logiciel/matériel, interaction des parties mécaniques), la fiabilité de certains blocs peut être modélisée avec un arbre de panne, et par conséquent l'information résultant sur la probabilité d'apparition de ces blocs peut être attribuée à ce bloc spécifique faisant partie du bloc-diagramme de fiabilité. De cette manière, les blocs-diagrammes de fiabilité, qui normalement présument de l'indépendance des défaillances des composants dans un bloc, donneront une prédiction plus réaliste.

6 Développement et évaluation

6.1 Considérations générales

6.1.1 Vue d'ensemble

Un arbre de panne constitue une représentation graphique organisée des conditions ou des facteurs produisant ou contribuant à produire un événement indésirable défini, appelé «événement de tête». Cette représentation est établie sous une forme clairement compréhensible, analysable et, si nécessaire, adaptable pour faciliter l'identification:

– des facteurs affectant la fiabilité et d'autres caractéristiques de performance du système. Ces facteurs, par exemple, incluent des déficiences de conception, d'environnement ou de contraintes fonctionnelles, de modes de panne de composant, de fautes des opérateurs, de pannes de logiciel ;

– des événements communs qui peuvent contribuer à plus d'une issue d'événements intermédiaires dans un arbre de panne. Par exemple, des événements communs influant sur plus d'un composant fonctionnel et qui pourraient annuler le bénéfice apporté par les redondances spécifiques ou influer sur deux ou plusieurs parties d'un produit, qui peuvent autrement sembler non liées d'un point de vue opérationnel.

L'analyse par arbre de panne est une méthode d'analyse déductive (descendante) qui a pour but de faire apparaître les causes ou les combinaisons de causes qui peuvent produire l'événement de tête défini. Cette analyse peut être qualitative, Méthode A, ou quantitative, Méthode B, en fonction de la portée des analyses.

Dans les cas où la probabilité d'apparition des événements de base ne peut pas être estimée, une AAP qualitative, Méthode A, peut être utilisée pour rechercher les causes d'issues défavorables potentielles avec des événements de base individuels et portant une indication descriptive de la probabilité d'apparition telle que: «fortement probable», «très probable», «probabilité moyenne», «probabilité éloignée», etc. comme expliqué en 5.1.

Une AAP quantitative, Méthode B, peut être utilisée, lorsque les probabilités d'événements de base ou primaires sont connues. Les probabilités d'apparition de tous les événements intermédiaires et de l'événement de tête (issue) peuvent ensuite être calculées en utilisant les expressions mathématiques appropriées.

6.1.2 Concepts et combinaisons d'événements et états

L'issue finale d'un arbre de panne (événement de tête) peut être une panne, ou un événement. Ici, l'arbre de panne décrit une panne ou un événement résultant des événements y contribuant ou autres pannes. Dans l'analyse de l'arbre de panne certaines combinaisons d'événements peuvent être des états ou des événements, alors que les autres doivent correspondre à l'issue. Par exemple, les entrées dans une porte OR où l'issue est un état ou un événement, peuvent être des états ou des événements. Toutes les entrées dans une porte AND qui telle une issue est un événement, doivent être des événements, alors que, si telle l'issue, elle représente un état, toutes les entrées doivent être des états.

L'état peut être caractérisé par la probabilité que cet état existera à l'instant *t*, alors que l'événement peut être caractérisé soit par le taux de défaillance ou la fréquence de défaillance, ou par la probabilité d'apparition à l'instant *t*.

6.1.3 Arbre de panne pour recherche de pannes menant aux autres pannes ou événements

Traditionnellement, un arbre de panne est construit pour la recherche de pannes ou d'événements menant à une issue. Ce concept a été utilisé depuis longtemps dans de nombreuses industries, et est particulièrement efficace et appliqué dans l'industrie nucléaire. De cette manière, il devient un outil puissant et une aide inestimable pour la recherche de problèmes potentiels, d'événements, d'améliorations et autres mesures préventives qui empêchent ou atténuent une issue indésirable.

Une issue, un succès ou une panne, est étudiée, et les états ou événements menant à cette issue étudiée, leur probabilité d'existence ou d'apparition est déterminée, et le modèle d'arbre de panne construit de façon appropriée, mènerait à la probabilité de l'existence ou de l'apparition de l'issue présumée.

Dans cette application, l'arbre de panne est construit et évalué comme décrit à l'Article 7 en gardant à l'esprit que l'issue est caractérisée par la probabilité d'existence de panne ou d'apparition d'événement, et n'est pas reliée à la fiabilité de l'élément analysé ou d'un système.

Il est possible que les bases ou les autres événements dans ce genre d'analyse ne reçoivent pas de valeur de probabilité réelle, et soient utilisés uniquement dans la recherche d'un événement qui peut potentiellement prendre place (Méthode A) . Dans ce cas, ils peuvent porter une indication descriptive de la probabilité «haute, moyenne ou basse» et sont évalués comme éléments de contribution potentiels à l'événement de tête ou à la panne. De tels types d'arbres de panne sont souvent utilisés pour l'identification d'une panne primaire ou événement qui était l'unique ou le principal élément contribuant à la panne de tête ou événement, et sont utilisés dans une grande variété d'industries. Automobile, nucléaire, usines de fabrication, etc.

6.1.4 AAP utilisée dans l'évaluation de la fiabilité et l'amélioration pendant le développement du produit

Dans cette application qui est basée sur la Méthode B de l'AAP, un arbre de panne peut modéliser le produit complet, ou des parties d'un produit qui peut présenter un risque pour sa fiabilité ou sécurité de fonctionnement. Dans ce cas, la probabilité d'apparition de l'analyse Méthode B peut être déterminée de manière traditionnelle, telle que dans l'analyse d'une panne ou événement d'un produit, lié à la sécurité, ou l'analyse détaillée d'une défaillance d'un produit potentiel sur une certaine durée peut conduire à l'expression de sa fiabilité insuffisante ou probabilité de défaillance sur la période concernée. Dans cette application, la méthodologie de l'arbre de panne suit les principes des modes de défaillance descendants et les analyses d'effets, où chaque mode de défaillance potentiel peut résulter en un événement ou une panne menant à la défaillance du produit.

L'AAP convient particulièrement dans ce cas, étant donné que la modélisation peut refléter les dynamiques des événements dans un produit, interaction logiciel/matériel, de même que l'interaction entre les pannes ou événements représentant les modes de défaillance potentiels. Il n'est pas possible de représenter cette interaction dans une FMEA régulière, et elle est très difficile à modéliser en utilisant les blocs-diagrammes de fiabilité traditionnels. De plus, les estimations de fiabilité du produit sont plus réalistes, étant donné que seuls les modes de défaillances qui contribuent à la défaillance d'un produit, comme défini, sont considérés.

Il est recommandé de commencer à construire l'arbre de panne dès les premiers stades de la conception et de poursuivre à chacune des étapes du développement. Il convient que l'évolution de l'arbre de panne soit telle qu'elle reflète les progrès de la conception: cela permettra de mieux comprendre les modes de défaillance au fur et à mesure de la conception. L'«analyse concurrente de la conception» permet de modifier très tôt la conception du système. De nombreux arbres de panne seront très ramifiés et un logiciel d'analyse par arbre de panne pourra alors être nécessaire pour les traiter. Il existe des logiciels qui facilitent l'analyse et permettent des estimations simples et rapides de la probabilité d'apparition de l'événement de tête. Il y a de nombreux programmes de logiciel AAP disponibles et peut être beaucoup plus en création. Ils ont tous suffisamment de différences pour répondre aux besoins de chaque utilisation spécifique.

Il est important de noter que les événements portés sur l'arbre de panne ne se limitent pas à des défaillances de logiciels ou de matériels, mais qu'ils comprennent leur interaction et d'autres facteurs, par exemple les facteurs humains ou les actions et les processus qui ont un rapport avec l'événement de tête.

Lorsqu'une analyse quantitative est réalisée, mais que la probabilité d'apparition de certains événements ne peut être déterminée, même si les pannes ou événements (défaillances) sont systématiques, il convient d'inclure ces événements et leur combinaison (logique) fonctionnelle dans l'analyse. Dans ce cas, ces modes de défaillance ne seront pas pris en compte dans la prédiction de fiabilité (ou probabilité de défaillance) mais leur existence est prise en compte de toute façon de manière qualitative.

Pour utiliser efficacement la technique de l'arbre de panne comme méthode d'analyse d'un système, il convient que la procédure comprenne au moins les étapes suivantes:

– définition de la portée de l'analyse;
– familiarisation avec la conception, les fonctions et le fonctionnement du système;
– définition de l'événement de tête;
– construction de l'arbre de panne;
– analyse de la logique de l'arbre de panne;
– rapport sur les résultats de l'analyse;
– évaluation des améliorations de la fiabilité et arbitrages.

Si une analyse numérique est planifiée, il sera nécessaire de définir une technique pour une évaluation numérique des probabilités d'événement primaire ou autres attributs tels que l'intensité de défaillance, la durée moyenne de fonctionnement entre les défaillances (MTBF) d'évaluation ou la durée moyenne de fonctionnement avant défaillance (MTTF), etc. La sélection de la donnée à utiliser et de l'évaluation numérique des mesures de fiabilité ou non-fiabilité sortent du domaine d'application de cette norme.

Il y a de multiples objectifs dans l'AAP de conception d'un système. L'une de ses applications est la modélisation de l'architecture et de la fonctionnalité du produit de façon descendante, à la recherche des modes de défaillance potentiels et de leurs causes et qui peuvent produire une issue défavorable, telle que définie par l'événement de tête. En se basant sur cette information, qui contribue à la probabilité d'apparition de l'événement de tête ou à l'insuffisance de fiabilité du système (à la fois quantitativement et qualitativement pour identifier les causes) et poursuit la recherche jusqu'à l'identification de leurs causes respectives. Cela permet un arbitrage et des études pour des solutions possibles à la réduction de modes de défaillances potentiels, et finalement une évaluation de l'amélioration de la fiabilité obtenue.

L'AAP étant un modèle de l'architecture et de la fonctionnalité du produit, il convient qu'elle soit effectuée par des personnes possédant une connaissance détaillée du système, de ses caractéristiques de conception et de son fonctionnement, et formées à l'AAP et aux autres techniques de modélisation de fiabilité correspondantes. L'analyste doit être capable d'évaluer les influences des modes de défaillance potentiels et d'identifier logiquement les causes possibles d'une telle anormalité dans la performance du produit. Un manque de connaissance en ingénierie de conception du produit et des modes de défaillance potentiels conduiront à une AAP qui pourra ne pas être une représentation réelle de la fonctionnalité du produit et, par conséquent, les résultats analytiques n'auront pas de sens. Au moment de sa préparation, il convient que l'AAP soit revue par l'équipe d'ingénierie participant à la conception du produit en termes d'exactitude et d'exhaustivité. Il faut que les actions correctives décidées soient documentées et suivies.

6.2 Information du système exigée

Il convient que chaque système soit défini par une description de sa fonction et par une identification de ses interfaces. Il est recommandé que cette définition comporte les éléments suivants:

– un résumé des objectifs recherchés dans la conception;

– une définition de ce qui constitue une défaillance du système;

– une structure fonctionnelle du système généralement représentée par un bloc-diagramme fonctionnel;

– les limites du système, comme les interfaces électriques, mécaniques et fonctionnelles, dépendront de l'interaction et des interfaces avec d'autres systèmes. Il convient de décrire ces limites en identifiant les fonctions particulières, par exemple les connexions électriques (interne ou externe), les fusibles, qui constituent les interfaces;

– la structure matérielle du système, par opposition à sa structure fonctionnelle;

– l'identification des modes de fonctionnement et une description du fonctionnement du système ainsi que de ses performances attendues ou acceptables, pour chaque mode de fonctionnement;

– le profil de fonctionnement du système;

– les conditions relatives à l'environnement du système et les aspects humains pertinents (c'est-à-dire le degré de formation pour les opérateurs et le personnel de maintenance), etc.;

– une liste des documents à prendre en compte, par exemple, plans, spécifications, manuels de fonctionnement, qui contiennent une description détaillée de la conception et du fonctionnement du matériel. Il convient que la durée des missions, les intervalles entre les essais (périodiques), le temps disponible pour les actions de maintenance corrective, soient connus, ainsi que le matériel auxiliaire et le personnel nécessaires. Des informations spécifiques sur les fonctions exigées pour chaque phase de fonctionnement sont également requises.

6.3 Structure et description graphique de l'arbre de panne

Les composants d'un arbre de panne sont les suivants:

Portes:

– Symboles montrant la relation logique entre les événements d'entrée et l'événement de sortie
  – portes statiques – issue ne dépendant pas de l'ordre d'apparition des entrées
  – portes dynamiques – issue ne dépendant pas de l'ordre d'apparition des entrées

Le tableau décrivant les portes dynamiques et les commentaires sur leur utilisation se trouve à l'Annexe A, Tableau A.3. Un exemple de porte PAND est représenté à la Figure A.1.

Evénements:

– Niveau d'entrée le plus bas dans un arbre de panne. Les symboles d'événements couramment utilisés et leur définition sont présentés à l'Annexe A, Tableau A.1.

Les composants graphiques d'un arbre de panne sont les suivants:

a) un symbole logique dans un arbre de panne (portes);
b) des lignes d'entrée des portes;
c) des descriptions de l'événement intermédiaire;
d) des symboles de transfert vers l'intérieur ou l'extérieur ;
e) des symboles d'événements primaires.

Il convient d'inclure dans l'arbre de panne tous les événements pertinents. Il est recommandé que ces événements incluent les effets des conditions d'environnement ou d'autres conditions de contraintes, auxquels l'entité peut être soumise, y compris le logiciel, les contrôles et la surveillance des statuts, ceux que l'on peut rencontrer pendant le fonctionnement, même s'ils ne sont pas prévus dans les spécifications relatives à la conception.

Il convient que les événements que l'analyste a étudiés, mais qu'il a écartés pour la suite de l'analyse parce qu'il les a considérés comme ne devant pas être pris en compte, soient signalés dans le rapport mais non portés sur l'arbre de panne définitif.

Si l'arbre de panne révèle deux ou plusieurs problèmes dans le fonctionnement du système dû(s) à une panne existante, il convient alors que l'événement correspondant à cette panne soit porté en de multiples endroits sur l'arbre de panne. Il convient de signaler cet événement comme un événement commun. Dans l'analyse qualitative, les événements communs sont inclus dans les calculs une fois pour toute et il convient d'appliquer tous les critères de disjonction montrés en 7.5.5.4. Afin d'éviter une introduction accidentelle de tels événements répétés dans de multiples calculs, il convient d'établir et d'utiliser un libellé conventionnel d'événements. Le type de libellé doit être cohérent. Si un logiciel est utilisé pour l'assistance d'évaluation de l'arbre de panne, des conventions et des jeux appropriés doivent être utilisés.

Les arbres de panne créés peuvent être représentés à la verticale, de haut en bas, à l'horizontale de gauche à droite. Si l'arbre de panne est représenté à l'horizontale, tous les symboles des Tableaux A.1 à A.4 seront tournés à 90° dans le sens des aiguilles d'une montre.

Les arbres de panne peuvent aussi se lire ou s'étudier dans des directions opposées, par exemple en traitant d'accidents survenus, de défaillances, etc.

7 Elaboration et évaluation de l'arbre de panne

7.1 Généralités

Le développement d'un arbre de panne commence à la définition de l'événement de tête. L'élaboration d'un arbre de panne dans son application traditionnelle ou pour une analyse de la fiabilité de système ou du mode de défaillance est une méthode déductive dans laquelle l'analyse débute à partir de l'événement de tête indésirable tel qu'il est défini comme objet de l'analyse. Une fois élaboré comme prévu, l'arbre de panne devient une représentation graphique de tous les événements qui contribuent, par eux-mêmes ou avec d'autres événements, à l'apparition de l'événement de tête.

7.2 Portée de l'analyse

Pour définir la portée de l'analyse, il convient de préciser quel est le système à analyser, l'objectif et l'étendue de l'analyse ainsi que les hypothèses de base. Il est recommandé d'inclure dans ces hypothèses celles qui concernent les conditions prévues de fonctionnement et de maintenance ainsi que le fonctionnement du système dans toutes les conditions d'utilisation possibles.

L'AAP peut donner des informations sur

– l'analyse de fiabilité du système, dans les cas où la probabilité d'apparition des événements primaires est connue ;

– la cause première d'une issue défavorable qui a eu lieu, qui peut nécessiter une action corrective appropriée.

Le domaine d'application de l'AAP s'étend à un système complexe lorsque la probabilité d'apparition d'un événement de tête doit être déterminée. Ici, contrairement à d'autres modélisations de fiabilité et méthodes analytiques de prédiction, le domaine d'application d'analyse s'étend uniquement pour inclure les modes de défaillances ou événements potentiels qui influent sur le fonctionnement du système, c'est-à-dire, uniquement les modes de défaillance qui sont pertinents pour l'apparition de l'événement de tête. Cela entraîne ensuite une évaluation de la fiabilité du système plus ciblée, qui peut être mieux comparée à la performance en exploitation.

7.3 Approfondissement de la connaissance du système

Pour réussir une analyse par arbre de panne, il faut posséder une connaissance approfondie du système. Cependant, certains systèmes peuvent être trop complexes pour qu'une seule personne puisse posséder pleinement cette connaissance. Dans ce cas, pour se familiariser avec le système, il est nécessaire que les compétences spécifiques soient réunies au sein d'une équipe.

7.4 Elaboration de l'arbre de panne

L'élaboration de l'arbre de panne commence par la définition de l'événement de tête ou issue défavorable qu'il convient de définir sans ambiguïté. L'événement de tête est le point sur lequel est centrée toute l'analyse. Il peut s'agir de l'apparition ou de l'existence d'une condition dangereuse (analyse de sécurité) ou de l'incapacité du système à fonctionner comme prévu.

Si, dans l'analyse de performance ou de fiabilité d'un système, un événement de sortie d'une porte définit l'incapacité à réaliser une fonction, les événements d'entrée correspondants peuvent représenter des causes appropriées: par exemple, défaillance due à des pannes du matériel, des pannes du logiciel, des limitations des performances, une commande incorrecte (défaillance de contrôle), et à une erreur humaine.

L'élaboration d'une branche d'arbre de panne particulière s'achève lorsqu'un ou plusieurs événements suivants ont été atteints:

– événements primaires, c'est-à-dire événements indépendants dont les caractéristiques à prendre en compte peuvent être définies par d'autres moyens qu'un arbre de panne;
– événements qui n'ont pas besoin, selon l'analyste, d'être développés plus avant pour le moment;
– événements qui ont été ou seront développés plus avant dans un autre arbre de panne – transfert. Si ces événements font l'objet d'une étude plus poussée, ils doivent avoir respectivement la même identification que les événements correspondant dans l'autre arbre de panne, de sorte que le deuxième arbre soit bien le prolongement du premier.

7.5 Construction de l'arbre de panne

7.5.1 Représentation de l'arbre de panne

Les arbres de panne peuvent être disposés soit verticalement soit horizontalement. Si l'on choisit la disposition verticale, il convient que l'événement de tête soit placé en haut de la page et les événements de base en bas. Dans le cas d'une présentation horizontale, l'événement de tête peut être situé à gauche ou à droite de la page.

Les exemples dans la norme (Figure 1 et autres) montrent le développement et la représentation d'un arbre de panne. En plus des symboles définis pour la logique de l'arbre de panne, les exemples contiennent la boîte de description de l'événement, de même que la fonction ou l'état représenté par l'événement.

7.5.2 Utilisation de l'AAP quantitative (Méthode B) dans le système ou développement de produit pour l'amélioration de la fiabilité

7.5.2.1 Généralités

L'AAP est une manière systématique pour identifier des événements qui contribuent à l'apparition de l'événement de tête et avec l'application de méthodes déductives, aux événements intermédiaires et finalement aux événements primaires. Cette analyse systématique identifie les modes de défaillance des composants du système et les facteurs qui contribuent à leur propre probabilité d'apparition, par exemple les contraintes de fonctionnement ou d'environnement y compris les commandes des logiciels, les facteurs humains, etc.

La première différence entre l'AAP et les autres méthodes d'analyse et de modélisation de fiabilité est que l'AAP comprend uniquement les événements qui contribuent à l'apparition de l'événement de tête, et modèle leur combinaison fonctionnelle et leur possible interdépendance et interaction dynamique, alors que les autres méthodes traitent les taux ou probabilité de défaillance des composants (non la probabilité du mode de défaillance du composant) avec l'hypothèse habituelle d'indépendance de défaillance. A titre d'exemple, un condensateur de filtrage de tension peut s'arrêter de fonctionner, en mode ouvert (environ 35 % de ses défaillances), en mode court (environ 55 % de ses défaillances) ou peut changer de capacité (les 10 % restant de ses défaillances), mais seule une défaillance en mode *court* serait la cause d'une défaillance du produit, alors uniquement 55 % environ de sa probabilité de défaillance est prise en compte. Cela permet une identification réaliste de ces modes de défaillance ou de leurs causes qui nécessitent l'attention du concepteur.

La capacité de l'AAP à modéliser correctement la séquence d'événements (avec l'assistance de l'analyse de Markov) primaires ou intermédiaires, comme entrée dans un autre événement intermédiaire en fait un outil instrumental pour identifier ces événements/fonctions primaires ou événements intermédiaires qui sont les éléments contribuant majoritairement à la non-fiabilité d'un produit. Cela permet des améliorations de la conception qui réduiront de telles failles dans la conception, et la révision de l'AAP pour vérifier l'amélioration ou pour réaliser l'étude de deux options d'amélioration ou plus.

Dans tous les modèles de portes suivants, il est important de garder en mémoire que les valeurs de probabilité sont celles des modes de défaillance et des facteurs qui y contribuent uniquement, ou sont les probabilités de ces combinaisons statiques ou dynamiques des modes de défaillance menant à la perte d'une fonction et à la défaillance du système.

L'utilisation de l'AAP de cette manière est expliquée en détail dans le «NASA Fault Tree Handbook with Aerospace Applications version 1.1», mentionné à l'Article 6.

7.5.2.2 Configuration du système en série

Dans les modèles de fiabilité, les assemblages (blocs ou composants dans le bloc-diagramme de fiabilité) sont dans une configuration en série dans un système où une défaillance de l'un d'entre eux peut conduire à la défaillance du système.

Le modèle correspondant dans l'arbre de panne serait que l'ensemble de ces «blocs» (portes ou événements) converge dans une porte OR.

La formule mathématique pour la fiabilité du «système» en tête, se composant de «n» blocs indépendants, serait la suivante:

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \cdot .....R_i(t) \cdot ....R_n(t) \quad (1)$$

Du point de vue de la fiabilité, l'expression ci-dessus signifie que le bloc 1 ***et*** le bloc 2, ***et*** le reste des blocs doivent être opérationnels pour que le système soit opérationnel.

Dans l'AAP, le contraire est utilisé. La défaillance est produite par la défaillance du composant 1 OU la défaillance du composant 2, et ainsi de suite. C'est la raison pour laquelle la porte OR représente un système en série ou une configuration d'assemblage.

La formule mathématique d'une porte OR est la même que celle présentée pour un système en série, mais exprimée en termes de probabilité de défaillance $F(t)$, qui est le complément probabiliste de la fiabilité.

$$F(t) = 1 - R(t) \quad (2)$$

La probabilité d'une issue défavorable d'une porte OR («système») se composant de n portes ou événements d'entrée indépendant(e)s est:

$$F_S(t) = 1 - (1 - F_1(t)) \cdot (1 - F_2(t)) \cdot ..... \cdot (1 - F_i(t)) \cdot ..... \cdot (1 - F_n(t)) \quad (3)$$

Le système est défaillant lorsque l'un des composants (blocs) est défaillant. Un exemple de porte OR est montré dans la Figure 2. Dans cette Figure 2 et dans toutes les suivantes de cet article, le mode de défaillance d'un composant en question est le mode de défaillance qui, comme événement d'entrée provoque l'apparition d'un événement de sortie.

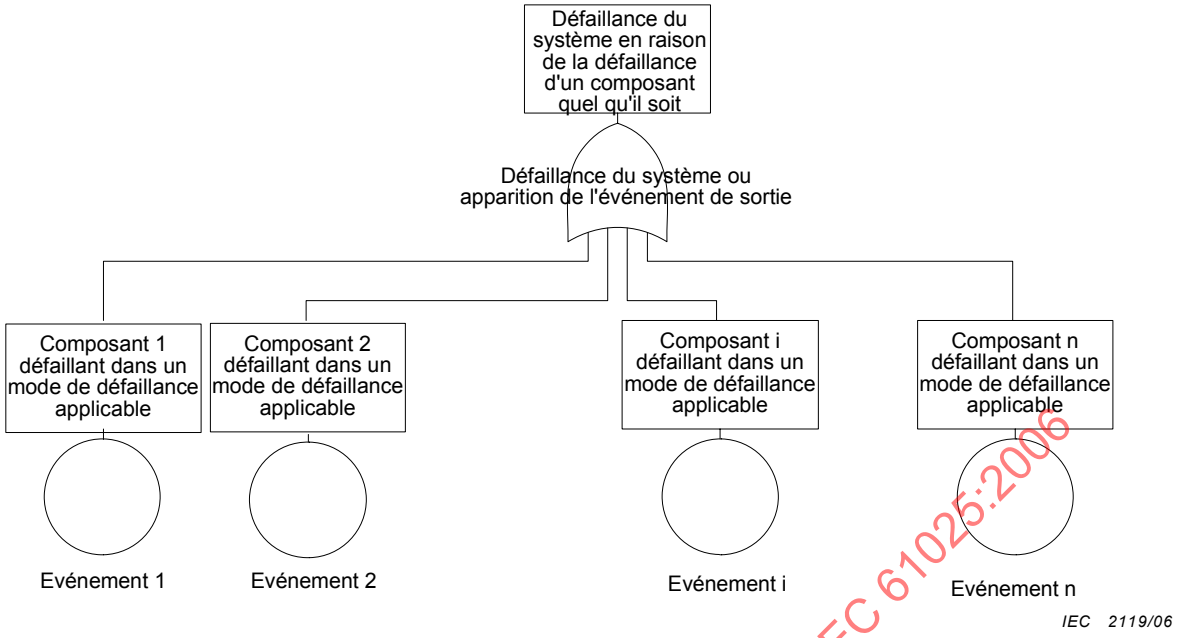


Figure 2 – Représentation de l'arbre de panne d'une structure en série

7.5.2.3 Configuration de système en parallèle, systèmes redondants

7.5.2.3.1 Redondance active

Le présent paragraphe suppose que les caractéristiques (modèles) de défaillance pour chaque entrée vers la redondance active restent les mêmes, indépendamment du nombre d'autres entrées qui fonctionnent. Il considère également que chaque entrée vers le bloc de redondance active est indépendante. Lorsqu'elle n'est pas indépendante, voir disjonction (Annexe B) pour des lignes directrices complémentaires.

Dans le cas d'un événement de sortie qui n'apparaîtrait que si tous les événements de contribution indépendants survenaient, ils devraient alors être liés par une porte AND. La configuration décrite peut être redondante. On s'y réfère aussi comme à un système parallèle pour l'analyse de fiabilité, bien que la configuration matérielle puisse être différente.

L'exigence d'indépendance est respectée lorsque la probabilité d'événements d'entrée ne change pas, quelque soit l'état des autres entrées.

L'expression mathématique associée en fiabilité est basée sur le fait que le système est opérationnel si le composant 1 OU le composant 2 OU l'un des composants, au moins l'un d'entre eux reste opérationnel, ce qui signifie que le système est défaillant si tous les composants sont défaillants.

$$R_S(t) = 1 - \prod_{i=1}^{n} \left(1 - R_i(t)\right) \tag{4}$$

Avec l'AAP, cela est représenté par une porte AND, ayant «n» portes ou événements d'entrée, avec la signification que le système est défaillant si le composant 1 ET le composant 2 ET le reste des composants sont défaillants, avec la même formule mathématique: Probabilité de défaillance:

$$F_S(t) = \prod_{i=1}^{n} \left(F_i(t)\right) \tag{5}$$

Dans l'AAP, une représentation de la redondance parallèle, dans laquelle un seul composant non défaillant est suffisant pour la réussite du fonctionnement du système, est présentée à la Figure 3.

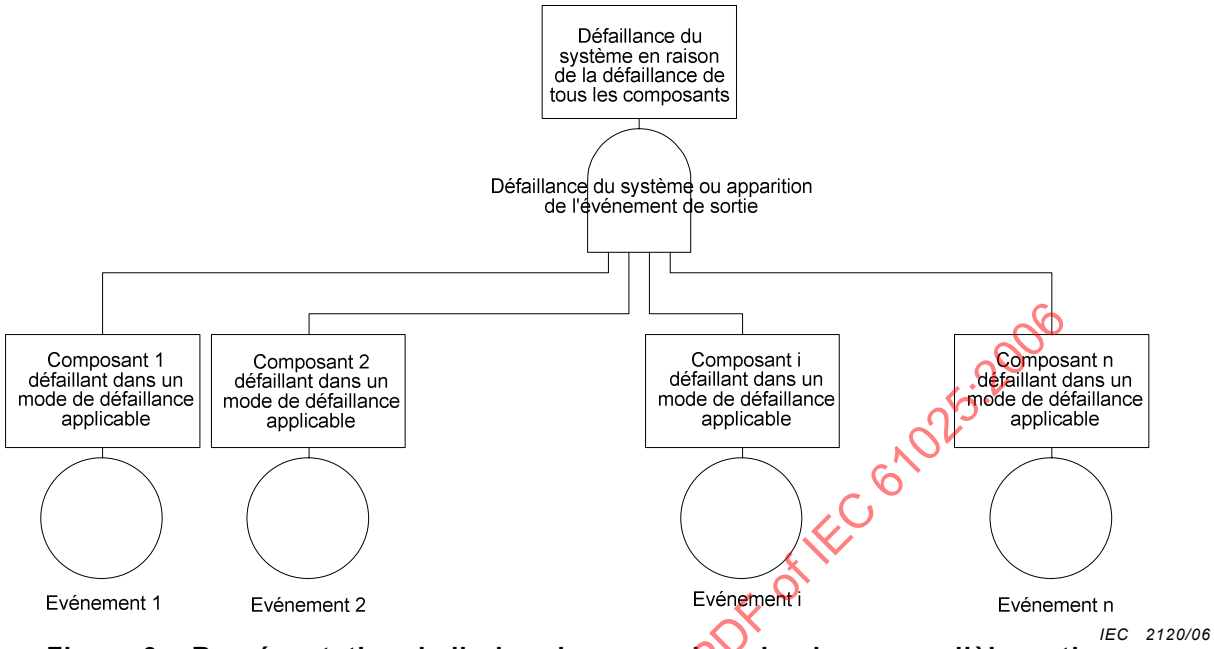


Figure 3 – Représentation de l'arbre de panne de redondance parallèle, active

Les composants redondants peuvent fonctionner sur un mode de partage de charge (par exemple les générateurs d'un réseau électrique), la probabilité d'événement de défaillance des composants survivants peut augmenter à chaque panne. De telles modifications dans la probabilité d'événement casseraient l'exigence d'indépendance pour l'utilisation d'une simple porte AND.

Lorsqu'une sortie ne survient que si tous les événements de contribution surviennent, mais que les événements d'entrée sont dépendants les uns des autres, on ne peut pas utiliser une porte AND. Dans ce cas, une porte dynamique est utilisée.

Lorsque la redondance est telle que la condition de succès du système est que k de n blocs identiques reste opérationnel, l'expression mathématique pour la non-fiabilité, comme utilisée dans l'AAP est la suivante:

$$R_S(t) = 1 - \sum_{i=0}^{k-1} \frac{n!}{i!\cdot(n-i)!} \cdot [R_0(t)]^i \cdot [1 - R_0(t)]^{n-i}$$

ou (6)

$$F_S(t) = \sum_{i=0}^{k-1} \frac{n!}{i!\cdot(n-i)!} \cdot [1 - F_0(t)]^i \cdot [F_0(t)]^{n-i}$$

Dans l'AAP, cette combinaison d'événements est représentée par la porte de vote majoritaire, où le nombre de vote est $m = n - k + 1$ et le symbole dans la porte correspondante, m désigne combien d'événements doivent prendre place pour que l'événement se propage dans l'arbre.

A titre d'exemple, si la redondance requise est de 3 sur 6, le vote majoritaire est de 4, c'est-à-dire que l'apparition de quatre événements d'entrée ne laisse que deux composants à l'état opérationnel, ce qui signifie que le système est défaillant étant donné que l'exigence indiquait que 3 composants sur 6 devaient être opérationnels.

La porte du vote majoritaire, de même que d'autres exemples de portes utilisés dans la modélisation de la fiabilité est présentée dans la Figure 4.

7.5.2.3.2 Redondance passive (en attente)

La redondance en attente est le cas où seul le nombre de composants requis pour le fonctionnement est actif, et en cas de défaillance de l'un ou de plusieurs de ces composants, un ou plusieurs composants de remplacement sont activés pour reprendre la fonction du composant défaillant. La défaillance du système est définie comme l'événement où un nombre inférieur au nombre total de composant opérationnel est inférieur au nombre requis pour le fonctionnement du système. Les composants redondants (de remplacement) dans l'analyse peuvent être considérés comme n'étant pas soumis à la défaillance (composants de remplacement froids), soumis à une certaine probabilité intermédiaire de défaillance (composants de remplacement chauds) jusqu'à ce qu'ils soient mis en fonctionnement actif, ou peuvent être soumis de la même manière à la défaillance, comme lorsqu'ils sont opérationnels (composants de remplacement brûlants).

La représentation de la redondance en attente n'est pas possible avec les portes statiques. Cependant, un symbole de porte SPARE peut être utilisé. L'analyse de Markov doit être utilisée pour analyser cette porte.

La redondance en attente est traitée avec succès par les arbres de panne dynamiques. Ici, la porte de remplacement est utilisée pour les systèmes redondants lorsque les probabilités d'événement changent.

7.5.2.4 Représentation d'événement répétés (cause commune) de probabilité conditionnelle, et événements de transfert extérieur

La probabilité d'un événement est conditionnelle lorsqu'elle dépend de l'apparition d'un autre événement, le deuxième événement ne survenant que si le premier événement a lieu.

La probabilité conditionnelle est également exprimée en termes de portes dynamiques qui utilisent l'analyse d'état de Markov, telles que les portes PRIORITY AND définies au Tableau A.4, Annexe A.

Un exemple de probabilité conditionnelle est présenté dans une partie de la Figure 4.

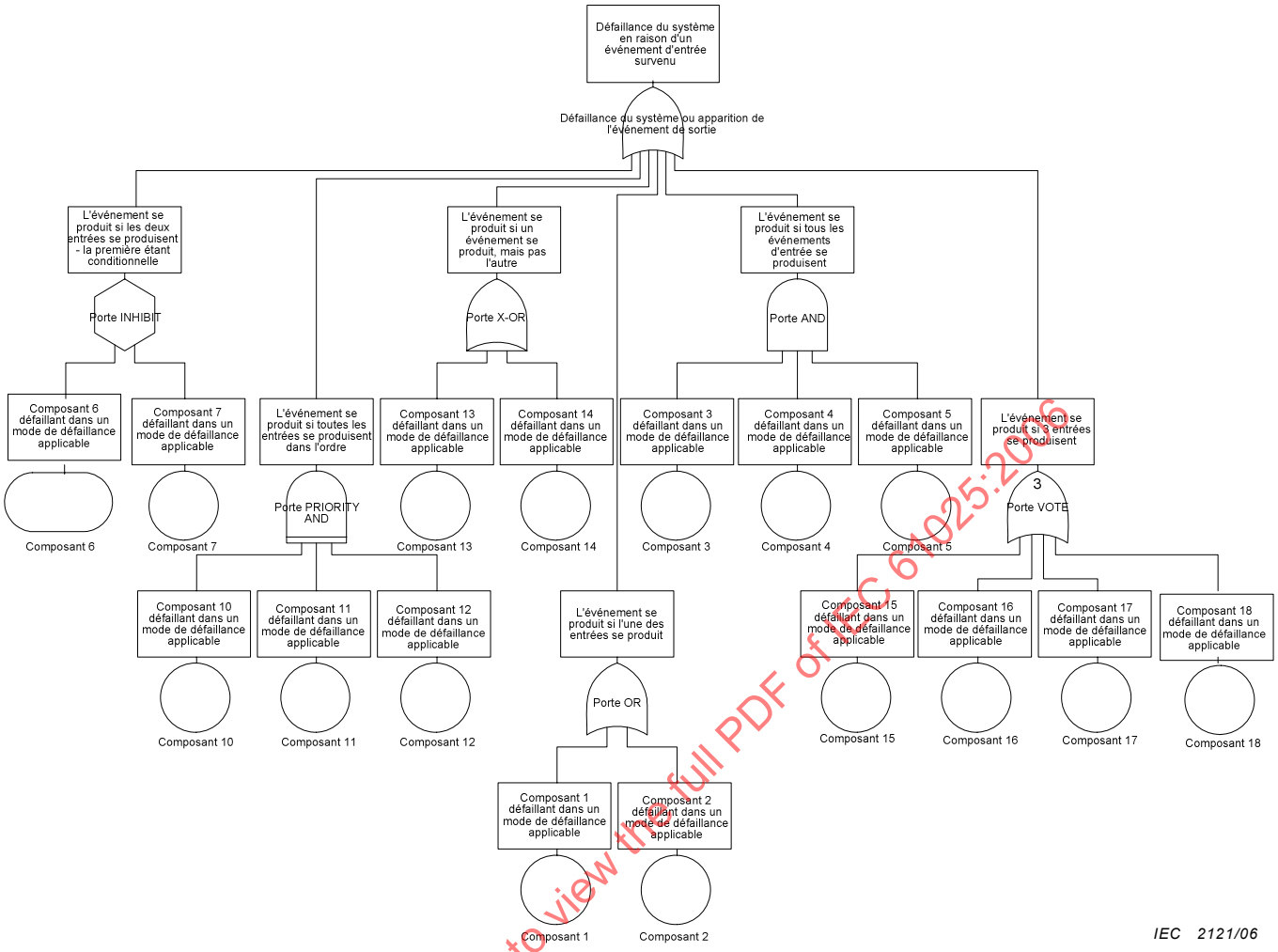


Figure 4 – Exemple d'arbre de panne montrant différents types de porte

Il convient de considérer la représentation graphique des arbres de panne montrée à la Figure 1 et les autres figures montrées dans cette norme, uniquement comme des exemples.

7.5.2.5 Représentation visuelle des arbres de panne

Les arbres de panne peuvent être représentés sous forme de différents graphiques, en fonction des préférences et de la représentation habituelle des différents pays et dans des applications différentes. Certaines représentations utilisent des formes rectangulaires avec des symboles à l'intérieur, tels que **&**, pour une porte AND, et **≥** pour la porte OR. Dans ce cas, la porte nulle est également classée comme porte OR, sauf si cette porte a seulement un événement d'entrée, les portes nulles représentant un événement de sortie ayant uniquement un événement d'entrée. Il faut prendre des précautions lors de la représentation des portes et des événements sous forme de rectangles, afin de s'assurer que les symboles à l'intérieur de ces rectangles sont bien définis et clairement marqués.

La représentation des portes et des événements rectangulaires est présentée à la Figure 5.

A la Figure 5, l'événement A ne se produira que si les événements B et C ont lieu. L'événement C ne se produira que si l'événement D ou E a lieu.

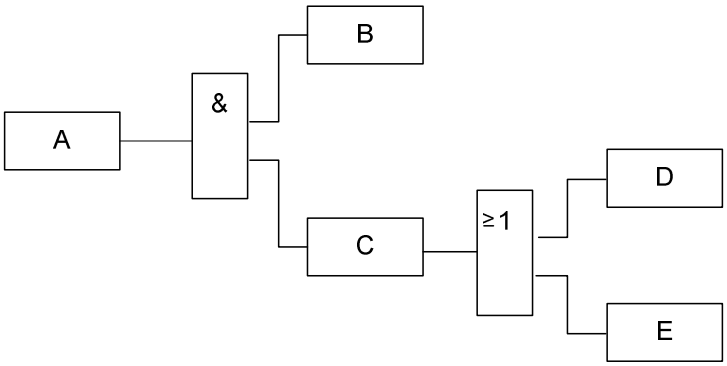


Figure 5 – Porte rectangulaire et représentation des événements

NOTE Pour chaque événement, A, B, etc., il est préférable de lister le nom ou la description de l'événement en premier, suivi du code de l'événement et de la probabilité d'apparition.

Si un événement représente un événement répété ou un événement de cause commune, il est montré dans l'arbre de panne à plusieurs reprises, mais avec un drapeau qui est aussi montré comme un événement d'entrée aux autres événements dans l'arbre de panne. Tous les événements répétés ou de cause commune dans cet ensemble doivent avoir le même code d'événement et être désigné par un symbole de report ou un symbole normalement utilisé comme tel dans un arbre de panne particulier. Cette règle s'applique à tous les événements répétés ou de cause commune sauf l'événement sur le niveau inférieur dans l'ensemble, qui est désigné par un symbole de report différé. Dans certains graphiques d'arbre de panne, les symboles pour les événements répétés de niveaux primaires ou plus élevés, sont les mêmes.

La Figure 6 montre un exemple ou une représentation graphique où l'événement répété, représenté comme une porte OR et avec le numéro de page en drapeau, est trouvé dans une autre place de l'arbre de panne, où il est un événement d'entrée d'un autre événement différent de niveau plus élevé. Cet événement peut se produire dans plus de deux places d'un arbre de panne. Un exemple d'un tel événement pourrait être l'élévation en température ou humidité causant l'apparition de deux événements différents dans un système. La disjonction est appliquée dans ce cas à un tel événement. De même, dans la Figure 6, on montre une porte de transfert pour indiquer que cet événement a été développé dans une autre place ou page d'un arbre de panne. Ceci est généralement le cas lorsqu'un événement plus complexe est un événement d'entrée d'un événement de niveau plus élevé, par conséquent il doit être développé plus avant sur un document séparé. Une porte PRIORITY AND montrée à la Figure 6, serait utilisée lorsque l'événement de sortie est dépendant de l'ordonnancement des événements d'entrée.

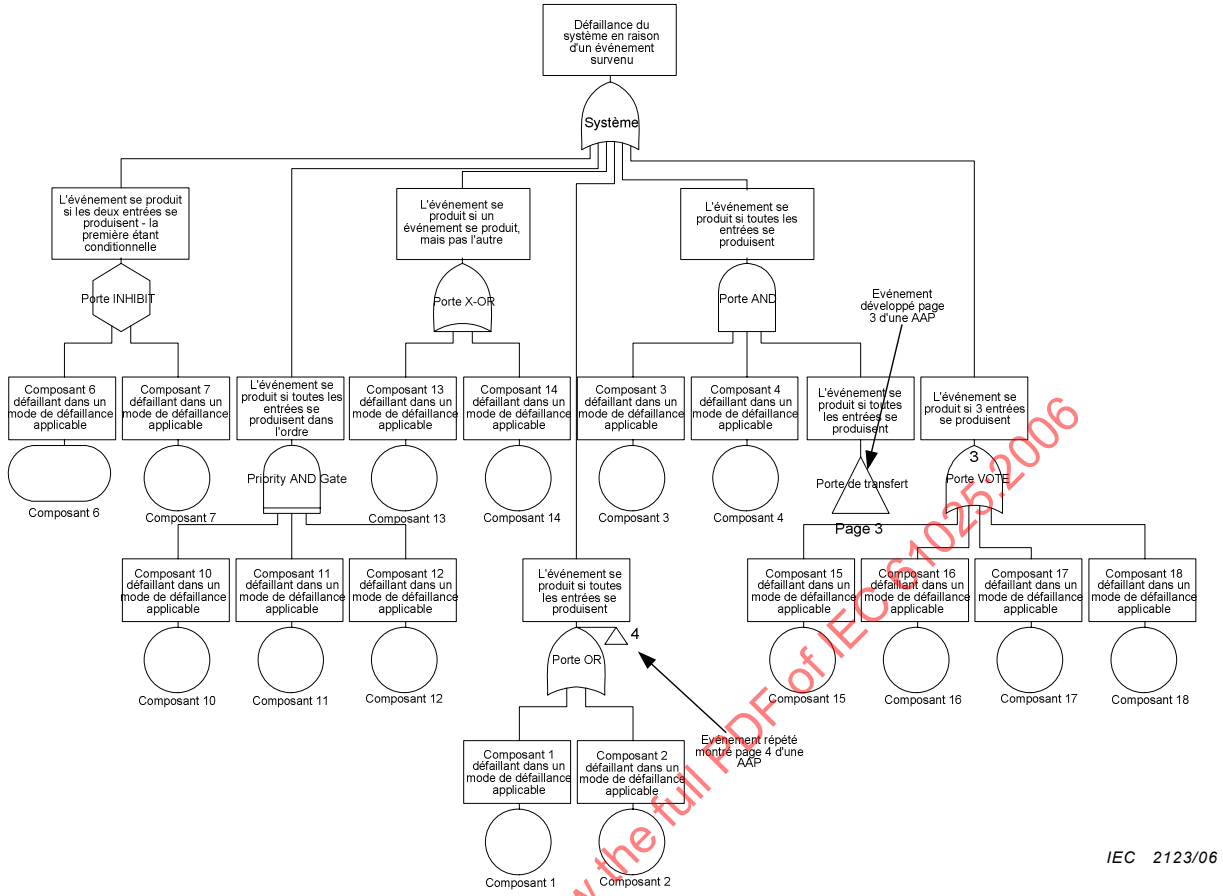


Figure 6 – Exemple d'arbre de panne contenant un événement de transfert et un événement répété

Un exemple d'arbre de panne rectangulaire montrant un événement de transfert extérieur ou de cause commune est visible Figure 7. L'événement B est un événement qui est analysé de manière plus poussée sur un autre arbre de panne. L'événement D est un événement de base.

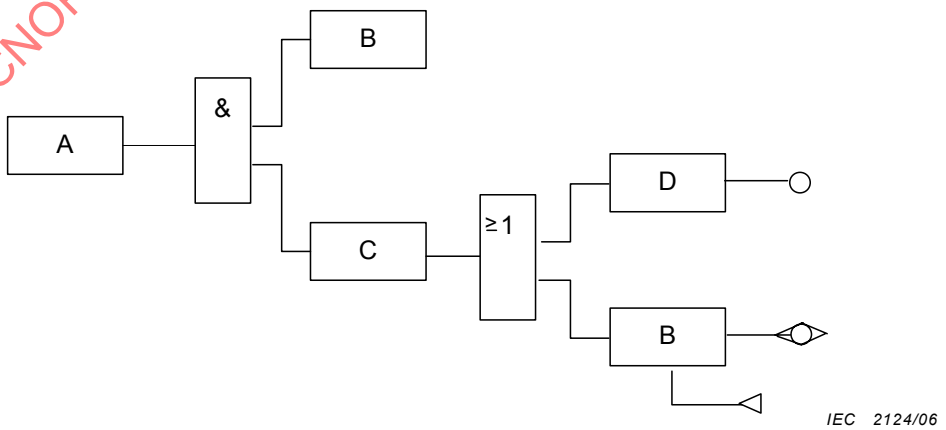


Figure 7 – Exemple présentant des indications se rapportant à une cause commune dans une représentation de porte rectangulaire

7.5.3 Technique de construction

La première étape dans la construction d'un arbre de panne est de définir clairement l'événement de tête, le domaine d'application et l'objectif de l'arbre de panne, les limites du système ou de l'objet de l'analyse et la résolution de l'analyse. Il convient que cet objectif soit défini en termes de définition de l'événement de tête.

Il faut que l'événement de tête décrive un problème qui doit être analysé pour en déterminer les causes. Dans l'application AAP pour l'amélioration de la fiabilité d'un système en développement, l'événement de tête est une défaillance du système et l'objectif de l'analyse est de déterminer ce qui contribue à cet événement et d'identifier les faiblesses de la conception ou les composants non fiables. Dans l'analyse quantitative la probabilité d'apparition de l'événement de tête et toutes ou la plupart des entrées seront déterminées. Dans l'analyse qualitative, Méthode A, les entrées de l'événement de tête seront examinées afin d'identifier les causes de leur apparition (autres événements ou pannes). Dans l'analyse quantitative, Méthode B, pour l'amélioration de la conception, les entrées de l'événement de tête sont analysées pour identifier les principaux éléments contribuant à l'événement de tête, et améliorer la conception par une élimination systématique de ces faiblesses ou réduction de ces modes de défaillances.

Le domaine d'application de l'analyse définit les événements ou les modes de défaillance qui seront inclus dans l'arbre de panne. Le domaine d'application couvre aussi les détails du problème analysé, le niveau de révision de la conception du système analysé, le profil d'utilisation du système et autres conditions fonctionnelles et environnementales, alors que les limites définissent ce qui est inclus et ce qui est exclu de ce système (par exemple, les connections internes, les enveloppes mécaniques, etc.).

Il convient de construire un arbre de panne de façon à ce qu'il représente clairement le flux d'événement qui ont mené à l'apparition de l'événement de tête.

Une fois l'événement de tête clairement défini de même que les limites du système et de l'analyse, alors la construction de l'arbre de panne en découle de haut en bas. L'événement de tête a des entrées et leur combinaison est modélisée et représentée par la porte appropriée. Les entrées dans l'événement de tête sont alors développées systématiquement pour être des résultats de leur propre événement d'entrée. Chacune des entrées, en descendant l'arbre de panne est développée séparément et ce développement est complété lorsque les événements primaires sont atteints.

La résolution spécifiera dans quelle mesure le système doit être analysé. A titre d'exemple, un système électronique peut être analysé jusque dans ses composants et leurs causes et modes de défaillances, ou à un niveau supérieur dans son assemblage (par exemple, processeur de signal, amplificateur de puissance, régulateurs de tension d'alimentation spécifique, etc.) Parfois, la résolution peut être une combinaison d'analyse de niveau détaillé et d'assemblage, liée à la disponibilité de la probabilité d'information de l'apparition.

Si l'on ne respecte pas strictement le concept de «cause immédiate» (événement d'entrée), on risque d'omettre des modes de défaillance en croyant les avoir déjà inclus.

Le concept d'«unité de base» permet à l'analyste de ne pas élaborer des branches d'arbre de panne qui n'apportent pas d'informations nouvelles ou utiles. Une unité de base n'est pas développée plus avant. Elle est traitée comme si elle était une unité ou un composant unique ou comme si elle était examinée séparément.

Pour qu'une unité ou un événement soit considéré(e) comme étant «de base», il faut et il suffit que les trois exigences suivantes soient satisfaites:

– les limites fonctionnelles et matérielles sont clairement définies;

– le fonctionnement de l'unité ne dépend d'aucune fonction auxiliaire ou bien tous les événements se rapportant à l'unité sont exprimés par une seule porte OR dont l'une des entrées représente une panne de l'unité, alors que les autres entrées représentent des incapacités à remplir les fonctions auxiliaires correspondantes;

– aucune cause immédiate ne peut être déterminée pour l'apparition de l'événement.

Il convient que la nomenclature utilisée dans un arbre de panne soit normalisée pour réduire la confusion et indiquer clairement ce que sont les événements de manière organisée.

La construction réelle d'un arbre de panne suit la logique analytique du flux des événements.

– Le concept de «cause immédiate» nécessite que l'analyste détermine les causes immédiates nécessaires et suffisantes à l'apparition d'une issue de tête. Il convient de noter qu'il ne s'agit pas des causes de base de l'issue de tête ou de l'événement de tête, mais des causes immédiates ou des mécanismes immédiats qui ont conduit à l'événement de tête. Ceux-ci peuvent être les événements (intermédiaires) de niveau inférieur.

– Les causes immédiates, nécessaires et suffisantes pour l'issue de tête sont maintenant traitées comme des événements intermédiaires, et l'analyse se poursuit pour déterminer les causes immédiates (événements d'entrée) nécessaires et suffisantes de ces événements.

– La construction progresse vers le bas de l'arbre de panne, en passant sans cesse du mécanisme au mode et en approchant continuellement le niveau inférieur du mécanisme et des modes, jusqu'au moment où le niveau approprié ou défini de résolution est atteint. Les événements de base individuels ou primaires (initiaux) sont ceux qui représentent les causes individuelles de défaillances ou de pannes potentielles.

7.5.4 Evaluation de l'arbre de panne

7.5.4.1 Investigation et analyse

L'investigation comprend l'étude de la structure de l'arbre de panne, par comparaison à des informations disponibles telles que des schémas, des dessins, des schémas fonctionnels, des commandes de logiciels, l'identification des événements de cause commune et la recherche des branches indépendantes. Il convient que l'investigation permette de dépister des événements de cause commune, mais qu'en aucune façon elle suppose que leur présence est insignifiante. De telles conclusions ne peuvent être tirées qu'après une analyse approfondie par réduction booléenne ou détermination de coupes minimales lorsque les portes statiques sont présentes, les coupes n'existant pas dans les portes dynamiques, à moins de faire une approximation pour ignorer la séquence. Comme la difficulté de l'analyse croît rapidement avec la taille de l'arbre de panne, l'investigation de l'arbre de panne aide l'analyste à savoir quelles branches sont indépendantes du reste de l'arbre et peuvent donc être analysées séparément si nécessaire.

L'analyse d'un arbre de panne suit le flux d'événements et identifie les causes de ces événements vers le bas. L'évaluation de l'arbre de panne peut être logique (qualitative) ou numérique (quantitative) ou les deux. L'analyse d'un arbre de panne quantitatif utilisée dans le développement de produit pour l'amélioration de la fiabilité identifie les facteurs qui contribuent fortement à la probabilité d'apparition de l'événement de tête, et les causes de celles ayant une probabilité d'apparition élevée. A titre d'exemple, si la probabilité de défaillance d'un assemblage d'un système contribue fortement à la probabilité de défaillance du système, la cause est recherchée et une fois identifiée, cette défaillance peut être atténuée. Pour illustrer cet exemple, un facteur contribuant à la probabilité de défaillance d'une alimentation électrique d'un système peut être identifié comme un condensateur sous contrainte excessive. Le remplacement d'un condensateur par un autre condensateur de tension plus élevée diminue considérablement la probabilité de défaillance de l'assemblage et, par la suite, du système.

Il convient que les documents fournis à l'appui des analyses soient présentés de sorte que l'on puisse revoir les résultats et incorporer toute modification jugée utile du fait de changements dans la conception, dans les procédures d'exploitation ou dans la meilleure compréhension des caractéristiques physiques de la défaillance. Pour cela, il est nécessaire que la construction puisse être effectuée de façon systématique. Une approche systématique implique la compréhension de deux concepts et leur emploi cohérent. Il s'agit des concepts de «cause immédiate» (événements d'entrée) et d'«unité de base».

Les analyses logiques (qualitatives) et numériques (quantitatives) d'un système ont essentiellement pour but:

– d'identifier les événements ou les pannes qui peuvent provoquer directement une défaillance du système, et contribuent à la probabilité de tels événements; et de cette manière, d'améliorer la sûreté de fonctionnement (fiabilité) d'un système;
– de réduire les pannes pouvant entraîner des conséquences qui peuvent être des dangers potentiels pour la sécurité;
– d'évaluer le niveau de défaillance toléré du système (capacité du système à continuer de fonctionner après la survenue d'un nombre donné de défaillances ou d'événements mineur(e)s conduisant à une défaillance du système);
– d'évaluer les données afin de pouvoir mettre en évidence les composants critiques et les mécanismes de défaillance;
– d'identifier les diagnostics de défaillance des dispositifs, les stratégies de réparation et de maintenance, etc.

Pour évaluer le niveau de défaillance toléré d'un système, il faut déterminer le degré de redondance dans le système et vérifier que des événements communs (événements de cause commune) ne nuisent pas à cette redondance. Bien que l'on n'ait pas besoin d'utiliser de données numériques pour ce type d'analyse, celles-ci sont nécessaires pour trouver les combinaisons d'événements qui ont le plus de chance de se produire et de provoquer une panne du système.

7.5.4.2 Analyse logique

7.5.4.2.1 Généralités

Il existe trois techniques fondamentales pour effectuer l'analyse logique: l'investigation, la réduction booléenne et la détermination de coupes minimales. La base de l'analyse logique est la modélisation, qui fournit une représentation d'arbre de panne d'une structure, fonctionnelle, architecturale, ou une combinaison des deux. Une modélisation correcte signifie une représentation des fonctions ou des composants d'un système, de manière à établir leurs interactions, dépendances, les causes immédiates d'issues défavorables, etc.

7.5.4.2.2 Réduction booléenne

La réduction booléenne peut être utilisée pour évaluer les effets des événements de cause commune (événements identiques apparaissant dans des branches différentes) dans les arbres de panne où l'événement de tête est indépendant de l'instant et de la séquence des événements. Pour procéder à une réduction booléenne, on peut résoudre les équations booléennes se rapportant à l'arbre de panne. La réduction booléenne peut également être utilisée pour identifier les coupes minimales.

7.5.4.2.3 Identification des coupes minimales

Il existe plusieurs méthodes permettant de définir les coupes minimales, mais elles peuvent être difficiles à appliquer à des arbres très ramifiés et, dans ce cas, elles risquent d'être à l'origine de lacunes. C'est pourquoi il existe divers programmes informatiques pour aider l'analyste dans sa tâche.

Une coupe est un groupe d'événements qui, lorsqu'ils se produisent conjointement, sont à l'origine de l'événement de tête. Une coupe minimale est le plus petit de ces groupes dont tous les événements doivent se produire pour que l'événement de tête ait lieu. Si l'un de ces événements dans une coupe minimale ne survient pas, l'événement de tête ne se produira pas. La définition peut être étendue à des arbres de panne qui dépendent de la séquence des événements. Dans ces cas, la coupe minimale définit le groupe d'événements qui peut être à l'origine de l'événement de tête. Quand l'apparition de l'événement de tête dépend de la séquence des événements d'entrée, cet événement est analysé en utilisant les techniques de Markov qui sont décrites dans la CEI 61165.

7.5.4.3 Analyse numérique

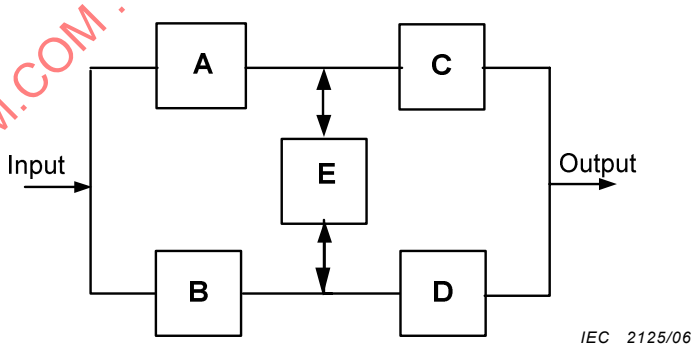
Cette analyse a pour but de parvenir à une estimation quantitative de l'apparition d'un événement de tête ou d'un ensemble choisi d'événements. L'analyse numérique peut également être utilisée comme aide et comme complément lorsqu'on effectue une analyse logique. Pour procéder à l'évaluation numérique d'un arbre de panne, on a besoin de données probabilistes sur les composants. Les techniques de prévision de fiabilité et de disponibilité, les résultats des essais ou les données recueillies en exploitation peuvent servir à déterminer les valeurs quantitatives.

7.5.5 Exemples d'une évaluation simple de matériel utilisant algèbre de Boole et sa représentation par un arbre de panne

7.5.5.1 Exemple de circuit à embranchement

L'arbre de panne avec l'algèbre de Boole peut simplifier l'analyse de fiabilité. Comme le montre cet exemple, les expressions mathématiques très complexes qui devraient être écrites si l'analyse était réalisée en utilisant un bloc-diagramme de fiabilité sont remplacées par l'algèbre de Boole considérablement plus simple. Bien entendu, l'utilisation de l'AAP est particulièrement adaptée aux circuits plus complexes où il existe également une interdépendance entre le logiciel et le matériel, et l'analyse est réalisée en utilisant un des nombreux progiciels.

Un exemple d'utilisation de l'analyse par arbre de panne pour la représentation d'un circuit à embranchement est représenté à la Figure 8.



NOTE Voir les Figures 11 et 12 pour les arbres de panne équivalents.

Figure 8 – Exemple de circuit à embranchement à analyser par arbre de panne

Dans le circuit à embranchement ci-dessus, le signal doit passer de l'entrée **'Input'** à la sortie **'Output'**. Il peut passer par le bloc E dans les deux directions. L'une des façons de réaliser l'analyse serait de modéliser le système selon deux circonstances possibles, tout d'abord en supposant que le bloc E est correct, puis en supposant que le bloc E est incorrect. Dans le premier cas, le signal passerait par les blocs A ou B et C ou D, comme s'il s'agissait de blocs parallèles, respectivement. Dans le cas où le bloc E est incorrect, (condition de défaillance de E) les blocs A et C sont en série, parallèles aux blocs B et D également en série. Cela est représenté par l'équation suivante: