

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



Analysis techniques for dependability – Event tree analysis (ETA)

Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre  
d'événement (AAE)

IEC 62502:2010

<https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010>



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland  
Email: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://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](http://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 It also gives information on projects, withdrawn and replaced publications.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](http://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](http://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](http://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](mailto: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](http://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](http://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](http://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](http://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](mailto:csc@iec.ch)

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



Analysis techniques for dependability – Event tree analysis (ETA)

Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre  
d'événement (AAE)

[IEC 62502:2010](https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010)

<https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX



ICS 21.020

ISBN 978-2-88912-212-7

# CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references .....	7
3 Terms, definitions, abbreviations and symbols.....	7
3.1 Terms and definitions .....	7
3.2 Abbreviations and symbols.....	8
3.2.1 Abbreviations .....	8
3.2.2 Symbols .....	9
4 General description .....	9
5 Benefits and limitations of ETA.....	11
5.1 Benefits.....	11
5.2 Limitations.....	11
6 Relationship with other analysis techniques.....	12
6.1 Combination of ETA and FTA .....	12
6.2 Layer of protection analysis (LOPA) .....	13
6.3 Combination with other techniques.....	13
7 Development of event trees.....	14
7.1 General.....	14
7.2 Steps in ETA .....	14
7.2.1 Procedure.....	14
7.2.2 Step 1: Definition of the system or activity of interest.....	15
7.2.3 Step 2: Identification of the initiating events of interest.....	15
7.2.4 Step 3: Identification of mitigating factors and physical phenomena.....	16
7.2.5 Step 4: Definition of sequences and outcomes, and their quantification.....	16
7.2.6 Step 5: Analysis of the outcomes.....	17
7.2.7 Step 6: Uses of ETA results.....	17
8 Evaluation .....	18
8.1 Preliminary remarks .....	18
8.2 Qualitative analysis – Managing dependencies.....	18
8.2.1 General .....	18
8.2.2 Functional dependencies .....	19
8.2.3 Structural or physical dependencies .....	20
8.3 Quantitative analysis .....	22
8.3.1 Independent sequence of events .....	22
8.3.2 Fault tree linking and boolean reduction .....	23
9 Documentation .....	24
Annex A (informative) Graphical representation .....	26
Annex B (informative) Examples .....	27
Bibliography.....	41
Figure 1 – Process for development of event trees .....	10
Figure 2 – Simple graphical representation of an event tree.....	18
Figure 3 – Functional dependencies in event trees .....	20

Figure 4 – Modelling of structural or physical dependencies.....	21
Figure 5 – Sequence of events .....	22
Figure 6 – Fault tree linking .....	23
Figure A.1 – Frequently used graphical representation for event trees .....	26
Figure B.1 – Event tree for a typical fire incident in a diesel generator building .....	28
Figure B.2 – Simplified event tree for a fire event .....	29
Figure B.3 – Level-crossing system (LX).....	31
Figure B.4 – ETA for the level-crossing system.....	33
Figure B.5 – Simple example .....	36
Figure B.6 – Fault Tree for the Failure of System 1 .....	36
Figure B.7 – Fault Tree for the Failure of System 2.....	37
Figure B.8 – Modified event tree .....	38
Figure B.9 – Event tree with "grouped faults" .....	39
Table A.1 – Graphical elements .....	26
Table B.1 – Symbols used in Annex B .....	29
Table B.2 – System overview.....	31
Table B.3 – Risk reduction parameters for accidents from Figure B.4 .....	34

iteh STANDARD PREVIEW  
(standards.iteh.ai)

IEC 62502:2010

<https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010>

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

# ANALYSIS TECHNIQUES FOR DEPENDABILITY – EVENT TREE ANALYSIS (ETA)

## 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 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 62502 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1380/FDIS	56/1389/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 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 stability 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.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

## **iTeh STANDARD PREVIEW** **(standards.iteh.ai)**

[IEC 62502:2010](https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010)

<https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010>

## INTRODUCTION

This International Standard defines the basic principles and procedures for the dependability technique known as Event Tree Analysis (ETA).

IEC 60300-3-1 explicitly lists ETA as an applicable method for general dependability assessment. It is also used in risk and safety analysis studies. ETA is also briefly described in the IEC 60300-3-9.

The basic principles of this methodology have not changed since the conception of the technique in the 1960's. ETA was first successfully used in the nuclear industry in a study by the U.S. Nuclear Regulatory Commission, the so-called WASH 1400 report in the year 1975 [31]<sup>1</sup>.

Over the following years, ETA has gained widespread acceptance as a mature methodology for dependability and risk analysis and is applied in diverse industry branches ranging from the aviation industry, nuclear installations, the automotive industry, chemical processing, offshore oil and gas production, to defence industry and transportation systems.

In contrast to some other dependability techniques such as Markov modelling, ETA is based on relatively elementary mathematical principles. However, as mentioned in IEC 60300-3-1, the implementation of ETA requires a high degree of expertise in the application of the technique. This is due in part to the fact that particular care has to be taken when dealing with dependent events. Furthermore, one can utilize the close relationship between Fault Tree Analysis (FTA) and the qualitative and quantitative analysis of event trees.

This standard aims at defining the consolidated basic principles of the ETA and the current usage of the technique as a means for assessing the dependability and risk related measures of a system.

<https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abc-48a5-90f7-043051f92f06/iec-62502-2010>

---

<sup>1</sup> Figures in square brackets refer to the bibliography.

## ANALYSIS TECHNIQUES FOR DEPENDABILITY – EVENT TREE ANALYSIS (ETA)

### 1 Scope

This International Standard specifies the consolidated basic principles of Event Tree Analysis (ETA) and provides guidance on modelling the consequences of an initiating event as well as analysing these consequences qualitatively and quantitatively in the context of dependability and risk related measures.

More specifically, this standard deals with the following topics in relation to event trees:

- a) defining the essential terms and describing the usage of symbols and ways of graphical representation;
- b) specifying the procedural steps involved in the construction of the event tree;
- c) elaborating on the assumptions, limitations and benefits of performing the analysis;
- d) identifying relationships with other dependability and risk-related techniques and elucidating suitable fields of applications;
- e) giving guidelines for the qualitative and quantitative aspects of the evaluation;
- f) providing practical examples.

This standard is applicable to all industries where the dependability and risk-related measures for the consequences of an initiating event have to be assessed.

[IEC 62502:2010](https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010)

### 2 Normative references

<https://standards.iteh.ai/catalog/standards/sist/55f87cfb-5abe-48a5-90f7-043051f92f06/iec-62502-2010>

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

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 61025:2006, *Fault tree analysis (FTA)*

### 3 Terms, definitions, abbreviations and symbols

For the purposes of this document, the following terms and definitions, as well as those given in IEC 60050-191, apply.

#### 3.1 Terms and definitions

##### 3.1.1

##### **node**

point in the graphical representation of the event tree depicting two or more possible outcomes for the mitigating factor

NOTE The top event of the corresponding fault tree can directly be linked to a node.

##### 3.1.2

##### **common cause**

cause of occurrence of multiple events

[IEC 61025:2006, 3.15]

**NOTE** Under particular circumstances the timeframe should be specified in which the multiple events occur, such as “occurrence of multiple events occurring simultaneously or within a very short time of each other”.

**EXAMPLES** Particular natural dangers (e.g. fire, flood), failures of an engineered system, biological infections or human acts.

### 3.1.3

#### **event**

occurrence of a condition or an action

[IEC 61025:2006, 3.8]

### 3.1.4

#### **headings**

listed mitigating factors in a line above the depiction of the event tree

### 3.1.5

#### **initiating event**

event which is the starting point of the event tree and the sequence of events that may lead to different possible outcomes

### 3.1.6

#### **mitigating factor**

system, function or other circumstantial factor mitigating the consequences of the initiating event

**NOTE** Many industries have specific equivalent terms, e.g. lines of defense, protection lines, protection systems, safety barriers, lines of assurance, risk reduction factor, etc.

### 3.1.7

#### **outcome**

possible result of the sequence of events after all reactions of relevant mitigating factors have been considered and no further development of the event tree is required

### 3.1.8

#### **sequence**

chain of events, from the initiating event, through subsequent events, leading to a specific outcome

### 3.1.9

#### **top event**

predefined undesired event which is the starting point of the fault tree analysis, and is of primary interest in the analysis. It has the top position in the hierarchy of events in the fault tree

**NOTE** It is the outcome of combinations of all input events.

### 3.1.10

#### **branch**

graphical representation of one out of two or more possible outcomes originating from a node

## 3.2 Abbreviations and symbols

### 3.2.1 Abbreviations

CCA	Cause-Consequence Analysis
ETA	Event Tree Analysis
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
IRF	Individual Risk of Fatality

LESF	Combination of two dependability techniques: Large Event Trees (LE) with connected Small Fault Trees (SF)
LOPA	Layers Of Protection Analysis
RBD	Reliability Block Diagrams
PRA	Probabilistic Risk Assessment
PRA/PSA	Probabilistic Risk/Safety Analysis
SELF	Combination of two dependability techniques: Small Event Trees (SE) with connected Large Fault Trees (LF)

### 3.2.2 Symbols

$A$	When used in italics, an upper case letter indicates that the event $A$ has occurred.
$\overline{A}$	When used in italics with a bar, an upper case letter indicates that the event $A$ has not occurred.
$I_E$	When used in italics, this indicates that the initiating event has occurred.
$O_{I_E, A, B}$	This denotes the outcome which results, if all of the events in the subscript (with upper case letters in italics separated by commas) have occurred in the order of the events stated in the subscript (see an example in Figure 3).
$\alpha, \dots, \delta$	Lower case Greek letters denote particular outcomes of the event tree.
“+”	This symbol denotes a logical “OR”.
“.”	This symbol denotes a logical “AND”.
$P(A)$	Probability of an event $A$ . $P(A)$ is a real number in the closed interval $[0, 1]$ assigned to an event, see [25].
$P(I_E . A . \overline{B} . \overline{C})$	Probability that the initiating event $I_E$ has occurred and event $A$ has occurred and event $B$ has not occurred and event $C$ has not occurred.
$P(A   I_E)$	Conditional probability of event $A$ given that the initiating event $I_E$ has occurred.
$f$	Frequency (the number of events per unit of time, see [25]).
$f_\delta$	Frequency of outcome $\delta$ .

## 4 General description

Event tree analysis (ETA) is an inductive procedure to model the possible outcomes that could ensue from a given initiating event and the status of the mitigating factors as well as to identify and assess the frequency or probability of the various possible outcomes of a given initiating event.

The graphical representation of an event tree requires that symbols, identifiers and labels be used in a consistent manner. Since the representation of event trees varies with user preference, a collection of commonly used graphical representations is given in Annex A.

Starting from an initiating event, the ETA deals with the question "What happens if...". Based on this question, the analyst constructs a tree of the various possible outcomes. It is therefore crucial that a comprehensive list of initiating events is compiled to ensure that the event trees properly depict all the important event sequences for the system under consideration. Using

this logic, the ETA can be described as a method of representing the mitigating factors in response to the initiating event – taking into account applicable mitigating factors.

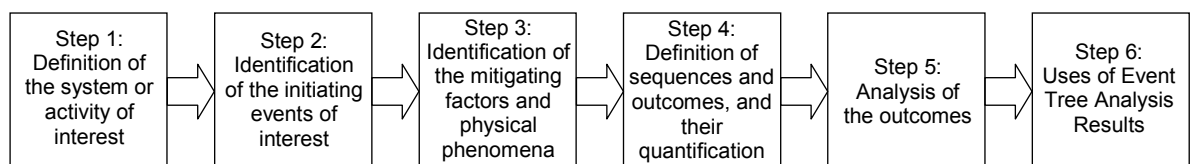
From the qualitative point of view, ETA helps to identify all potential accident scenarios (fanning out like a tree with success- or failure-branches) and potential design or procedural weaknesses. The success branch models the condition that the mitigating factor is operating as intended. As with other analysis techniques, particular care has to be taken with the modelling of dependencies, bearing in mind that the probabilities used for quantifying the event tree are conditioned on the event sequence that occurred prior to the occurrence of the event concerned. Clause 8 deals with these qualitative aspects of the analysis as well as the basic quantitative rules for the calculations required to estimate the (dimensionless) probabilities or frequencies (1/h) of each of the possible outcomes. Though one could, in theory, model the effect of failures of the operator or software by an event tree, this standard does not deal with their quantification since these issues are covered by other IEC publications, e.g. IEC 62508 [23] and IEC 62429 [22].

The advantages of ETA as a dependability and risk-related technique, as well as the limitations, are discussed in Clause 5. As an example of the limitations of ETA, the time-dependent evolution has to be considered cautiously because it can be handled properly only in particular cases. This limitation has led to the development of strongly related methods such as the dynamic event tree analysis method, which facilitate the modelling of time-dependent evolutions. This dynamic event tree analysis method will not be detailed in this standard; however, references are included in the bibliography for further information.

ETA bears a close relationship with FTA whereby the top events of the FTA yield the conditional probability for a particular node of the ETA. This is explained more fully in Clause 6 which also covers the relationships between ETA and other analysis techniques such as cause-consequence analysis (CCA) and layer of protection analysis (LOPA). CCA combines cause analysis and consequence analysis hence using deductive and inductive approaches. LOPA has been developed by the process industry as a special adaptation of the ETA.

Since the first steps and a well constructed approach are crucial for success, Clause 7 describes the development of the event tree, starting with a precise system definition. Furthermore, Clause 7 deals with the different aspects of the system (technical, operational, human and functional) as well as the depth of the analysis. Another important issue is the question of how to establish the list of relevant initiating events.

Figure 1 depicts the main steps in performing an ETA. Although seemingly a straightforward process, the analyst has to bear in mind that the construction of an event tree is very much an iterative process.



IEC 2293/10

**Figure 1 – Process for development of event trees**

Clause 9 briefly outlines the documentation required for the analysis and the results.

Annex A summarizes the most commonly used graphical representations for event trees. Annex B provides examples of ETA that highlight its application in numerous fields and provides guidance for conducting ETA.

## 5 Benefits and limitations of ETA

### 5.1 Benefits

ETA has the following merits:

- a) it is applicable to all types of systems;
- b) it provides visualization of event chains following an initiating event;
- c) it enables the assessment of multiple coexisting system faults (states causing inability to perform a required function, e.g. defect of a surveillance system) or failures (termination of the ability to perform a required function, e.g. the event of a valve being stuck open) as well as other dependent events;
- d) it functions simultaneously in the failure or success domain;
- e) it identifies end events that might otherwise not be foreseen;
- f) it identifies potential single-point failures, areas of system vulnerability, and low-payoff countermeasures. This provides for optimized deployment of resources, and improved control of risk through improved procedures and safety functions;
- g) it allows for identification and traceability of failure propagation paths of a system;
- h) it enables decomposition of large and complex systems into smaller more manageable parts by clustering it into smaller functional units or subsystems.

The strength of ETA compared to many other analysis and risk-related techniques is its ability to model the sequence and interaction of various mitigating factors that follow the occurrence of the initiating event. Thus the system and its interactions with all mitigating factors in an accident scenario become visible to the analyst for further risk evaluations.

### 5.2 Limitations

The following limitations associated with dependability analysis techniques in general also apply to ETA:

- a) the initiating events are not revealed by the analysis itself; it is an analytical task of the people involved in using the method to compile a comprehensive list of initiating events;
- b) it is the task of the people involved in the process to compile a comprehensive list of possible operating scenarios;
- c) hidden system dependencies might be overlooked leading to unduly optimistic estimates of measures related to dependability and risk;
- d) practical experience with the method as well as preceding system investigations are needed to address correct handling of conditional probabilities and dependent events.

Further limitations particularly applicable to ETA are listed below:

- e) time-dependent evolutions that involve time-dependence of the involved probabilities can be handled only if the relevant systems display a genuine constant probability or failure rate, or if, in the case of recovery and repair strategies, steady state unavailability is assumed to be reached quickly. This aspect is to be taken into account when dealing with periodically tested systems;
- f) another difficult aspect of time dependent evolutions that involve dynamic situations, e.g. the success criteria for mitigating factors vary depending on how the prior mitigating factors have performed. Usually a conservative assumption is made to reflect the situation;
- g) situations when being in a particular state for more than a specified time can result in a fault state. This state is difficult to model in an event tree (e.g. slow loss of air from a tire);
- h) dependencies in the event tree, e.g. due to dependencies between the initiating event and the mitigating factors, need careful consideration. However, there are few analysis

techniques that alone are suitable for handling of dependencies (dependent failures). The combination of FTA and ETA can prove beneficial for handling these aspects;

- i) although multiple sequences to system failure may be identified, the different magnitude of the accidents associated with particular outcomes may not be distinguishable without additional analysis; however, awareness of such a need is required.

## 6 Relationship with other analysis techniques

### 6.1 Combination of ETA and FTA

In practice, ETA is sometimes performed as a stand-alone analysis and in other cases in combination with FTA.

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 undesirable event. For further details see IEC 61025.

The combination of ETA and FTA overcomes many of the weaknesses of ETA, e.g. common cause failures in the quantitative analysis can be taken into account. Thus, the combination of ETA and FTA results in a powerful analytical technique for dependability and risk analyses.

The combination of ETA and FTA (sometimes referred to as Cause-Consequence Analysis (CCA), see [30] and [36]) is commonly used, e.g. FTA can be used to evaluate the frequency  $f$  of an initiating event in an ETA. Note also that the conditional probabilities of events in an event sequence are often calculated by FTA. One example where ETA and FTA are combined is the so-called PRA (Probabilistic Risk Assessment) made for a nuclear power plant.

In principle, the propagation of any initiating event can be analysed by ETA. However, in one or more cases, this may not be appropriate for some of the following reasons:

- a) the resulting trees may become very complex,
- b) it is sometimes easier to develop causal relationships rather than event sequences;
- c) there are often separate teams dealing with operational (e.g. rules of procedure) and technical analysis. However the interface and dependencies between the operational domain (e.g. rules of procedure, maintenance rules) and the technical domain (system under consideration) is not always clear at the beginning of the analysis. Thus for practical procedures, the potential events at the interface between the operational and technical domain are defined first. In particular, in safety applications, this is standard procedure, as usually single failures are ruled out by design, e.g. by employing fail-safe design, and so usually ETA should not lead directly to severe outcomes by a single failure without any further possible mitigating factors.

One can choose between two approaches for combining event trees and fault trees. One approach is the LESF approach. If the event tree tends to become unreasonably large, the SELF approach can be used.

In the LESF approach, the states of all systems that support the system being analysed, hereafter referred to as support systems, appear explicitly in the event trees. The top events of the fault trees have associated boundary conditions which include the assumption that the support systems are in the particular state appropriate to the event sequence being evaluated. Separate fault trees are used for a given system for each set of boundary conditions. These separate fault trees can be produced from a single fault tree that includes the support systems and that, before being associated with a particular sequence, is "conditioned" on the support system state associated with this sequence. This approach generates LESF that explicitly represents the existing dependences. Since they are associated with smaller fault trees, they are less demanding in terms of computer resources and computer program sophistication. However, the complexity of the event trees increases rapidly due to the combinatorial mathematics with the number of support systems and the

number of support system states that are explicitly depicted in the tree. Furthermore, the quantification process is more cumbersome and subject to possible omissions. An additional consideration is that the LESF approach does not explicitly identify what specific combinations of support system failures lead to system (also referred to as front line system) failures. A simplified example of such a large event tree is presented in Figure B.1. See [31] for more details.

In the SELF approach, event trees with the initiating event and the mitigating functions, performed by the various mitigating system as headings, are first developed and then expanded to event trees with the status of front line systems as headings. The front line system fault tree models are developed down to suitable boundaries with support systems. The support system fault trees may be developed separately and integrated at a later stage into the models for the front line system. This approach generates event trees that are concise and that allow for a synthesized view of an accident sequence. Furthermore, subject to the availability of computer programs, the small event trees may be more readily computerized. However, dependencies and the corresponding importance of support systems are not explicitly apparent. A theoretical example of such a small event tree is presented in Figure B.3. See [4] for more details.

## 6.2 Layer of protection analysis (LOPA)

LOPA is a particular standardized form of ETA, which is used as a simplified means for risk analysis tailored for a particular application environment. LOPA is organized in the form of a worksheet similar to the failure mode and effects analysis (FMEA); initiating events are recorded in rows and the different protection layers (representing the standardized mitigating factors) in columns. This means that any event sequence of a LOPA can also be treated as an ETA. For risk analysis purposes, severity (or damage) levels are also integrated into the worksheet.

Therefore, LOPA can be considered as an ETA with a restricted set of possible mitigating factors tailored to a particular application environment. It is predominantly used in the process industry. More details on LOPA can be found in [1] and [5].

## 6.3 Combination with other techniques

ETA may be combined with any other technique that is helpful for the derivation of the probability of the success or failure of the corresponding mitigating factors (e.g. Markov techniques or reliability block diagrams (RBD), see [16]), but in these cases, the other techniques only complement the ETA.

In cases of non-trivial or time dependencies of the system behaviour (see 8.3.2), one may resort to the Markov techniques if its other specific restrictions are taken into account. For further details, see [17].

Another closely related dependability analysis technique is the failure mode and effects analysis (FMEA), see [13], which is a formal, systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects on system performance. Generally, an FMEA helps to identify the severity of potential failure modes and to establish that the design includes mitigating factors to reduce failure probabilities of the respective system or function to an acceptable level. This may serve as a first step into the development of an event tree by identifying the crucial failures of a system as possible initiating events.

Markov modelling, RBD and FMEA are respectively standardized in IEC 61165 [17], IEC 61078 [16] and IEC 60812 [15].