IEC 62502

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Analysis techniques for dependability – Event tree analysis (ETA)

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

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 It also gives information on projects, withdrawn and replaced publications.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 62502

Edition 1.0 2010-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Analysis techniques for dependability – Event tree analysis (ETA)

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

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

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.

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][1].

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.

---

1 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.

2 Normative references

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).
$\alpha,\ldots,\delta$	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.
$P(A\mid I_E)$	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_δ	Frequency of outcome δ.

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.

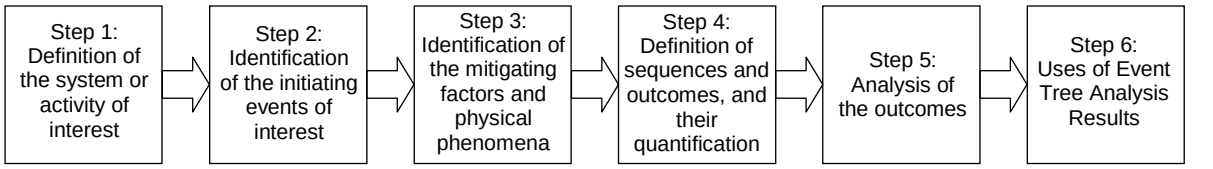

Figure 1 – Process for development of event trees

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].

7 Development of event trees

7.1 General

The events delineating the event sequences are usually characterized in terms of:

a) functions: the fulfilment (or not) of functions as mitigating factors;

b) systems: the intervention (or not) of systems as mitigating factors which are supposed to take action for preventing the progression of the initiating event into an accident or in the case of failure of the mitigating factors the mitigation of the accident itself;

c) phenomena: the occurrence or non-occurrence of physical phenomena.

Typically, the functions that are needed following an initiating event are identified first, and then the systems (mitigating factors) that can perform these functions. The physical phenomena describe evolution taking place inside and outside the system under consideration (e.g. pressure and temperature transients, fire, toxic dispersion, etc.).

The scope and purpose of ETA should be clearly defined before entering the detailed steps of 7.2.

7.2 Steps in ETA

7.2.1 Procedure

The procedure for performing ETA (see Figure 1) consists of the following six steps:

Step 1: Definition of the system or activity of interest (see 7.2.2)

Specify and clearly define the boundaries of the system or activity for which ETAs are to be performed.

Step 2: Identification of the initiating events of interest (see 7.2.3)

Conduct a screening to identify the events of interest or categories of events that the analysis will address. Categories include such things as collisions, fires, explosions, toxic releases, etc.

Step 3: Identification of the mitigating factors and physical phenomena (see 7.2.4)

Identify the various mitigating factors that can influence the progression of the initiating event to its outcomes. These mitigating factors include both engineered systems and human actions/decisions. Also, identify physical phenomena or circumstantial events, such as ignition or meteorological conditions that will affect the progression and finally the outcome of the initiating event. The event tree will be based on and constructed to include all of these mitigating factors and physical phenomena (see 7.1).

Step 4: Definition of sequences and outcomes, and their quantification (see 7.2.5):

For each initiating event, define the various outcomes (e.g. accident scenarios) that can occur and perform the actual quantitative analysis on the basis of the constructed event tree.

Step 5: Analysis of the outcomes (see 7.2.6)

The various outcomes are then analysed with respect to their consequences and their impact on the results of the analysis.

Step 6: Uses of ETA results (see 7.2.7)

The qualitative and quantitative findings of the analysis are then translated into necessary actions.

7.2.2 Step 1: Definition of the system or activity of interest

An ETA focuses on ways in which an initiating event can progress to accidents through the failures of various mitigating factors. A careful identification and investigation of mitigating factors is thus an important first step in evaluating the effectiveness of a mitigating factor.

Very few practical systems operate in isolation. Most are connected to or interact with other systems. By clearly defining the boundaries, in particular with support systems such as electric power and compressed air, analysts can avoid overlooking key elements of a system at interfaces, or penalizing a system by inadvertently associating other equipment with the subject of the study.

Conceptually, ETAs can include all of the events and conditions that can contribute to a specific outcome or can provide some level of protection against accidents of interest. However, it is not practical to include all possible contributions in the study. Many analyses define analytical boundaries that

a) limit the level of analysis resolution (e.g. the analyst may decide not to analyse in detail all electrical distribution system problems when studying a navigation system),

b) explicitly exclude certain types of events or conditions, such as sabotage, from the analysis.

The initial state of a system, including equipment assumed to be out of service initially, affects the combinations of events to result in subsequent outcomes. For example, if a protective interlock is routinely removed from service, the event tree will need to be modified so as to reflect the modified scenarios because of a potentially increased risk.

7.2.3 Step 2: Identification of the initiating events of interest

This step usually involves the use of a broad hazard identification technique, such as what-if, preliminary evaluation, or preliminary hazard analysis, to evaluate systematically all activities within the scope of the study, e.g. the consideration of the operational experience in the field of the specific industry. This step helps to identify the hazards and the possible initiating events that arise from these hazards. These identification methods broadly consider all operations within the scope of the study and seek to identify the full range of potential initiating events and the range of outcomes associated with such events. For an extensive list and description of various methods, see [12]. The outcome of these identification processes is usually an extensive list of potential events and their expected consequences.

It should then be the general aim to identify the entire spectrum of events that can occur within the scope of the analysis. After this has been done, the analysts apply screening criteria to identify the initiating events of most interest that will be considered in the event trees. Basically, there are two options for screening out initiating events, namely exclusion due to unlikely physical properties (e.g. specific values for pressure, temperature or fire loads are not exceeded) or due to low initiating event frequencies usually estimated in a conservative manner. This step helps identify those events that have to be analysed further to understand the complex interactions of systems. During this analysis one has to check the possibility of any interaction among initiating events and mitigating factors, e.g. whether the environment as caused by the initiating event, such as loss of all energy supplies after an earthquake, can adversely affect the performance of the mitigating factors.

After the initial list of events is identified and screened, the remaining list of initiating events includes those that will be considered in event trees. These are the events that are identified by experienced experts as complex enough to require additional analysis of the various system and personnel interactions that cause different outcomes from the initiating event.

If there are many events that will be considered in the event trees, the initiating events should be grouped into various categories, such as collisions, fires, explosions, toxic releases, etc. In some cases, this categorizing of events may not be applicable. For example, if the intent of the study is to identify the range of outcomes associated only with fires, then the screening

analysis performed in the previous step should have screened out all events that are not related to fires, so that this final step of categorizing the events is not necessary.

Initiating events which are grouped in the same class will require the intervention of the same mitigating factors and lead to similar outcomes.

7.2.4 Step 3: Identification of mitigating factors and physical phenomena

Once an initiating event is defined, all the mitigating factors that are required to mitigate the outcomes or accident scenarios shall be defined and organized according to their time of intervention. They consist of engineered components such as alarms, interlocks and automatic valves, and administrative or personnel systems, such as fire brigade, emergency response, and human detection through sight, sense of touch, sound, or smell.

The functions performed by the aforementioned components or mitigating factors are structured in the form of headings in the functional event tree. For each function, the set of possible successes and failures shall be identified and enumerated. Each set of successes or failures, respectively, associated with a mitigating factor gives rise to a branching of the event tree, not necessarily restricted to a two-branch node.

Physical phenomena, sometimes referred to as phenomenological events, can also influence the outcome of an initiating event. For example, if a flammable liquid is released, there may be engineered safety features to isolate the leak; however, if the leak is not isolated, the ultimate outcome of the release will be influenced by different physical responses, such as immediate ignition, delayed ignition, or dispersion characteristics. These physical responses are also modelled as nodes in the event trees.

In a system analysis requiring multiple event trees for multiple initiating events, the effort of drawing these event trees can be simplified by categorizing them according to the mitigating factors. This will allow the same event tree logic (i.e. mitigating factors with the same failure or success) to be repeated for different initiating events of interest. If the mitigating factors respond in an identical manner to various events, then the frequencies of the individual events can usually be summed to arrive at a representative frequency for all events of that class. For more details on the quantitative analysis, see 8.3.

7.2.5 Step 4: Definition of sequences and outcomes, and their quantification

As noted earlier, one of the strengths of the ETA technique is its ability to model the order of intervention and interaction of various systems that respond to the initiating event. Thus the intervention of the various systems can be modelled “one-after-the-other”. To account adequately for these interactions, the analyst has to

– determine the logical progression of the initiating event through the various mitigating factors to possible outcomes/accident scenarios,

– identify dependencies among the mitigating factors,

– account for conditional responses of one system, given the action of the previous systems,

– construct the event tree to address the above.

Certainly, not all initiating events (e.g. system failures) result in catastrophic outcomes. Similarly, not every mitigating factor or interlock is called upon to respond to every event that occurs. There is a logical progression to an accident sequence from the time the initiating event occurs. As the accident sequence progresses and becomes more severe, systems respond in different ways. Understanding the progression and timing of system and physical response is essential to developing the correct logic in the event tree. For example, if a fire ignites by spontaneous combustion in a waste receptacle, the initial response would be for personnel to extinguish the fire with handheld extinguishers, if personnel were present and there were extinguishers available. The full fire protection system and the response of the fire team would not be called upon unless the severity of the accident increased.

Most systems are connected to or interact with other items and processes. These interactions, or dependencies, will influence (degrade) the level of protection offered by redundant systems that share certain equipment. In the example of an oil tanker with redundant steering and propulsion systems, the failures of each system may not be independent if the steering systems shared a common hydraulic fluid supply.

Event trees involve conditional probabilities. That is, the probability of a specific response (e.g. success or failure) for a mitigating factor is conditioned on the specific response of the mitigating factors that precede it.

The recommended event tree construction process consists of the following steps:

a) place the initiating event first on the left side of the tree;

b) place the mitigating factors and physical phenomena across the top of the tree for instance in the chronological order in which they will affect the accident progression;

c) identify success (usually displayed in the upward branch) and failure (downward branch) of each mitigating factor at each node by considering the following:

   1) some nodes may have more than two outcomes and will be displayed with the appropriate number of branches (see Annex A);

   2) some nodes will have only one outcome; in other words, there is a straight line through that mitigating factor. This will occur when the conditional probability is 1,0; the mitigating factor does not affect the outcome because of some preceding success or failure of another mitigating factor.

These steps are illustrated in more detail in Annex A in general terms and more specifically in Figure B.1 and Figure B.4 with examples from the area of railway systems and power plants.

Quantitative analysis is presented in more detail in 8.3 and in an example in B.2.6.

7.2.6 Step 5: Analysis of the outcomes

The outcomes of ETA are determined by the end point of each event tree branch. Each outcome can be evaluated either qualitatively or quantitatively. In the former case, the outcome identifies various event sequences due to the occurrence of the investigated initiating event. The quantitative evaluation provides better insights on the relative importance of the mitigating factors because the outcome in that case is represented by a frequency. For quantifying ETA, adequate and sufficient reliable event occurrence data are needed.

It sometimes proves beneficial to split the possible outcomes into various categories according to the particular type of damage (loss of life, material damage, environmental damage or magnitude of damage, fuel damage). The number of outcomes of the event tree will be determined by definition of what types of outcome are to be analysed, e.g.

a) fault or damage states of the system;

b) destruction of the system;

c) severity of environmental impact; or

d) loss of human life.

For practical evaluation of the multiple outcomes to be assessed, it is useful to classify and group the outcomes, which are comparable, so as to simplify the results.

7.2.7 Step 6: Uses of ETA results

The results of ETA can be used to formulate a decision-making basis that may contribute to the selection of safety-wise optimum solutions for improving dependability and to reduce risk on a sound technical and organizational basis. The corrective actions may include changes to system architecture, operating and maintenance procedures, etc.

In particular, the decisions that are based on the performed analysis can be summarized as follows:

a) ability to assess risk tolerability or acceptability: the results taking into account the associated damage due to the relevant risk acceptability criteria are tolerable or not;

b) potential improvements: identify risk reduction factors and relevant changes to the system architecture under scrutiny in order to meet the acceptability criteria;

c) recommendations for improvement: develop specific suggestions for improving the performance, including any of the following

   1) equipment modifications,

   2) procedural changes,

   3) administrative policy changes such as planned maintenance tasks, personnel training, etc.

d) justification for the allocation of resources: estimate how implementation of the recommendations for improvement will affect the performance.

Since the analysed system may undergo changes over its lifetime, ETA should be kept up to date throughout the lifetime of the system to make it useful for the decision making process. This process of regular periodical updating is in some industries termed as 'living PRA/PSA' (Probabilistic Risk/Safety Analysis). The necessary embedding of the analysis in a general risk management process is described in more detail in [12].

8 Evaluation

8.1 Preliminary remarks

Before starting the quantitative analysis of the frequency or probability of the outcomes of the different event sequences, the qualitative aspects of the event tree model have to be analysed carefully. They contain the dependence of the events, including the initiating event and the top events as well as the intermediate or basic events of the linked fault trees.

In order to facilitate the depiction of the basic principles of the evaluation, the basic graphical representation of an event tree shown in Figure 2 is used for illustration purposes.

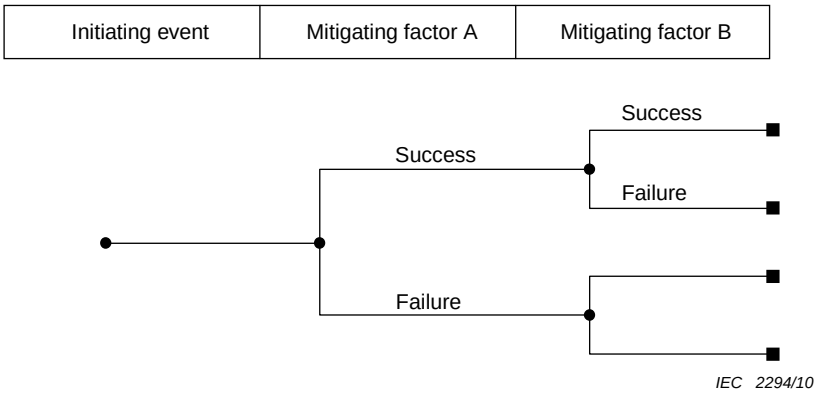

Figure 2 – Simple graphical representation of an event tree

8.2 Qualitative analysis – Managing dependencies

8.2.1 General

The objectives of the qualitative analysis can be summarized as follows:

a) to gain understanding of the factors that might determine dependence between functions or between the components of the system;

b) to identify the important potential dependent failure events;

c) to facilitate the correct quantitative analysis of the event tree and to establish the proper link with the fault trees.

The qualitative analysis and, in particular, the analysis of the dependencies, is covered in separate clauses in order to give the subject special emphasis, not because it has to be performed separately from event sequence analysis and system analysis.

There are two major aspects of dependencies, namely:

– functional dependencies (see 8.2.2);

– structural or physical dependencies (see 8.2.3).

For instance, the dependencies can be functional if the failure of a mitigating factor to intervene renders the intervention of the successive one impossible, for example, if the mitigating factors share some common component so that malfunctioning of that component puts them both out of operation. Further details on this distinction can be found in [40].

For simplicity, the event trees that follow are considered at the system level.

8.2.2 Functional dependencies

The ordering of the various mitigating factors in the event tree sequence is not only governed by their time of intervention as possible mitigating factors but also by their logic order. It has to be taken into account whether a successful intervention of one mitigating factor is dependent on the successful intervention of another. This could be the case, for instance, if

a) one mitigating factor represents a support system for the other, or

b) changes in the environmental parameters occur in such a way that the success or failure of the other mitigating factor is affected.

For example, consider the event tree shown in Figure 3 where the subsequent failures of the systems A and B (mitigating factors) lead to the outcomes shown. In this example, system A is supported by system B.

After a reordering of the systems A and B in the event tree (see Figure 3), the branch following the failure of system B does not need further decomposition in two branches for system A, because failure of system B implies system A cannot perform its function. This allows for the so-called pruning of the event tree. Since this is mostly done by computer programs, the main contribution of the analyst is to consider the various dependencies of the model.

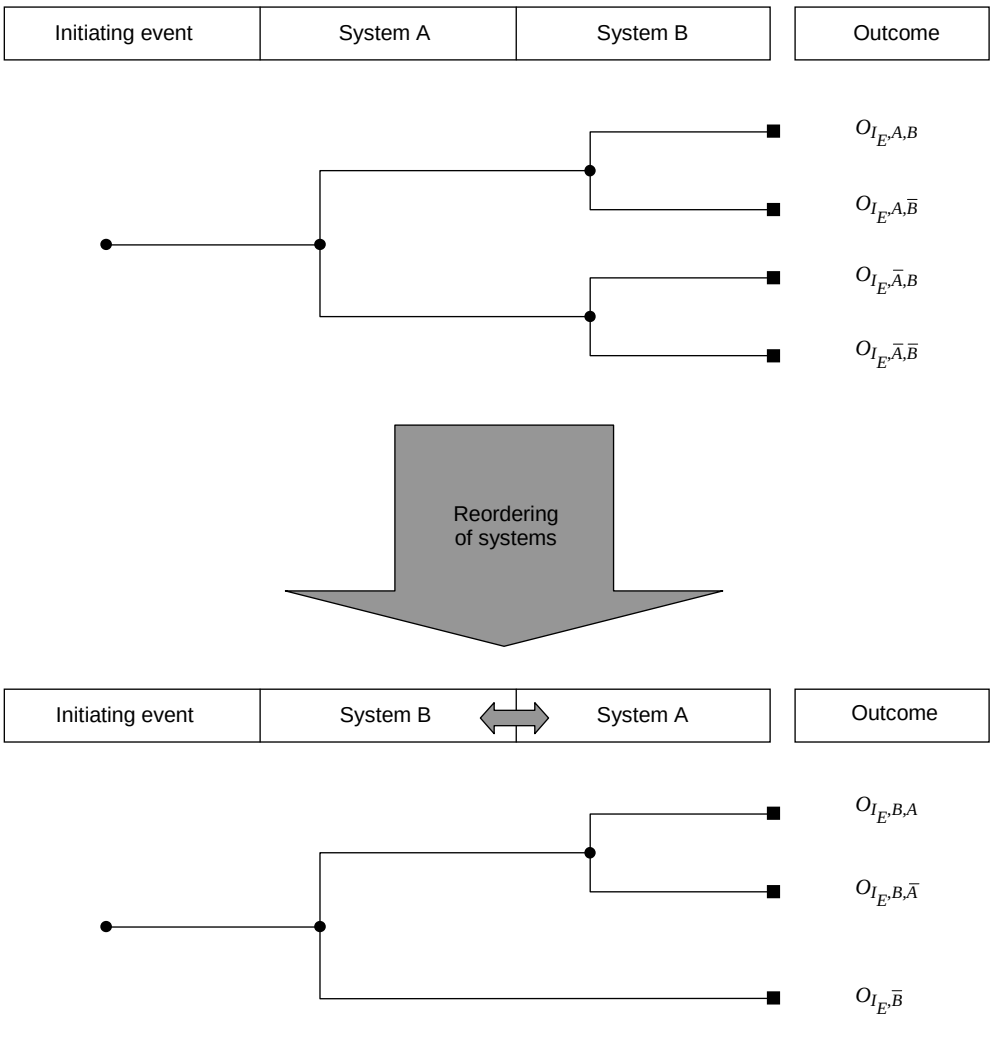

Figure 3 – Functional dependencies in event trees

Before applying the reordering process, one has to bear in mind that the depiction of the event tree may model a particular time sequence of the failure of the systems. Thus the particular event tree does not model the complete realm of possible time sequences after the initiating event. This has to be taken into consideration once the tools of fault tree linking or Boolean methods (8.3.2 and Clause B.2) are applied.

8.2.3 Structural or physical dependencies

Structural or physical dependencies generally result in common cause failures and such failures result in multiple events (see definition 3.1.2). Examples of common cause failures are those that are caused by events such as fires, earthquakes, hurricanes, failures of engineered systems (e.g. a massive electrical power failure or explosions – either internally or externally initiated), or human acts such as human errors, or acts of sabotage.

Therefore a common-cause analysis is carried out so as to determine the susceptibility of the various mitigating factors to failure from external or internal conditions, systems or functions.

One aspect to be clarified is whether the occurrence of the initiating event (e.g. an earthquake) affects the conditional probabilities of occurrence of all top events of the linked fault trees (see 8.3.2).

Another step of the qualitative analysis consists of identifying the common systems or common functions which influence the various mitigating factors. Consider, for example, an event tree where the failure of system A followed by a failure of system B leads to the undesired outcome. If system A relies on parts of system B to operate properly in order to function successfully, one could extract the “common part” and consider three systems: system A* and system B*, which are the systems A and B without the common parts, and system C, which represents the common parts used by both systems A and B. This scenario is depicted in Figure 4.

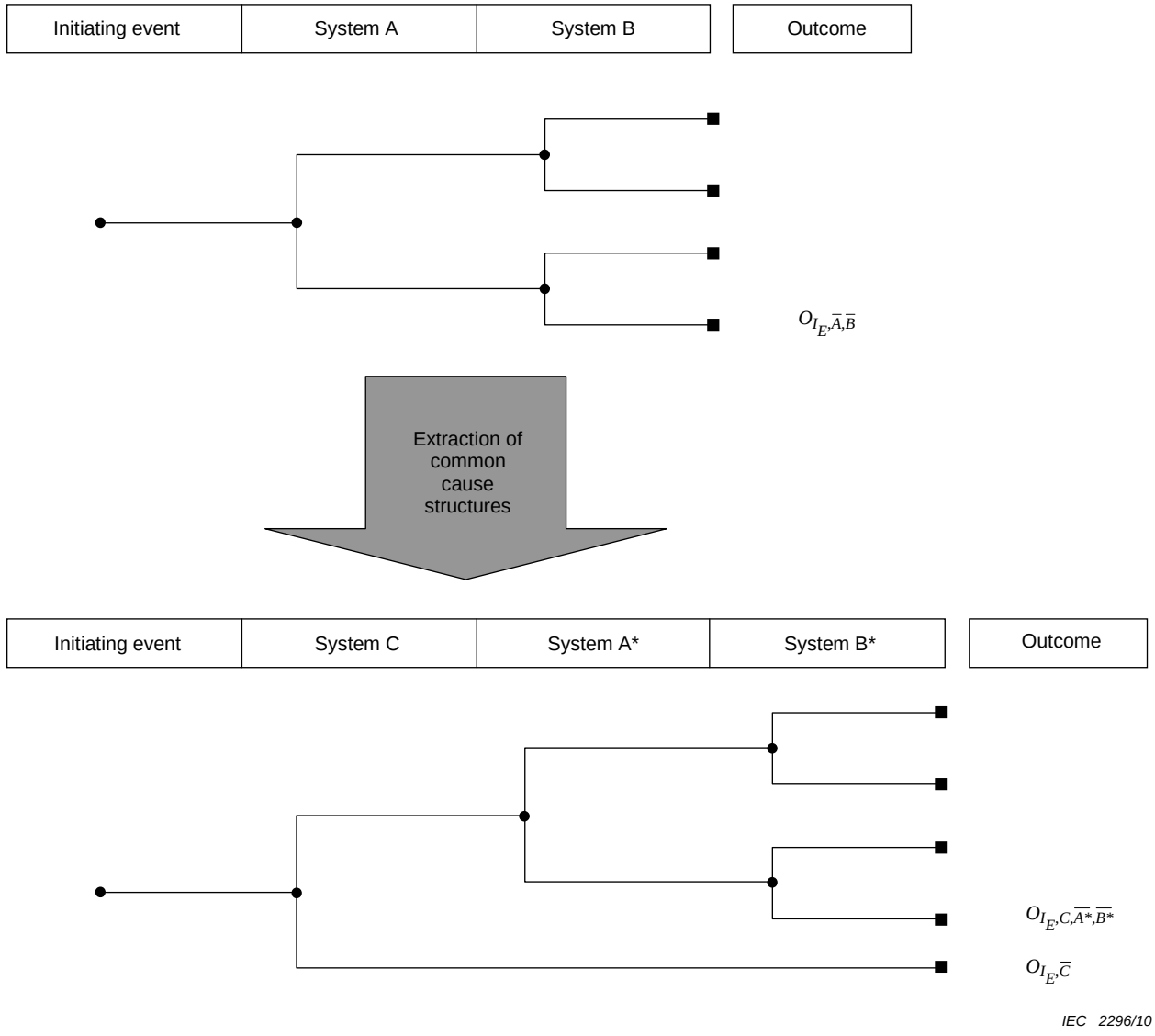

Figure 4 – Modelling of structural or physical dependencies

In most cases, the dependencies are much more complex than those illustrated above.

For instance, the failures caused by maintenance actions which are performed by members of the same maintenance teams cannot be modelled easily as depicted above. In the case of multiple combinations of dependent systems and their components, one can resort to the so-called fault tree linking, which is described in detail in 8.3.2.

8.3 Quantitative analysis

8.3.1 Independent sequence of events

When all the conditional probabilities of success or failure of mitigating factors are independent of one another, the quantitative analysis becomes very simple.

Consider an event tree with the three mitigating factors – systems A, B and C. Figure 5 depicts a particular sequence in the resulting event tree (illustrated by dotted line), where system A is functioning whereas systems B and C have failed. The following paragraphs explain the basic principles of evaluating the frequency or probability of the outcome of this particular sequence δ. Practical examples of event trees are given below.

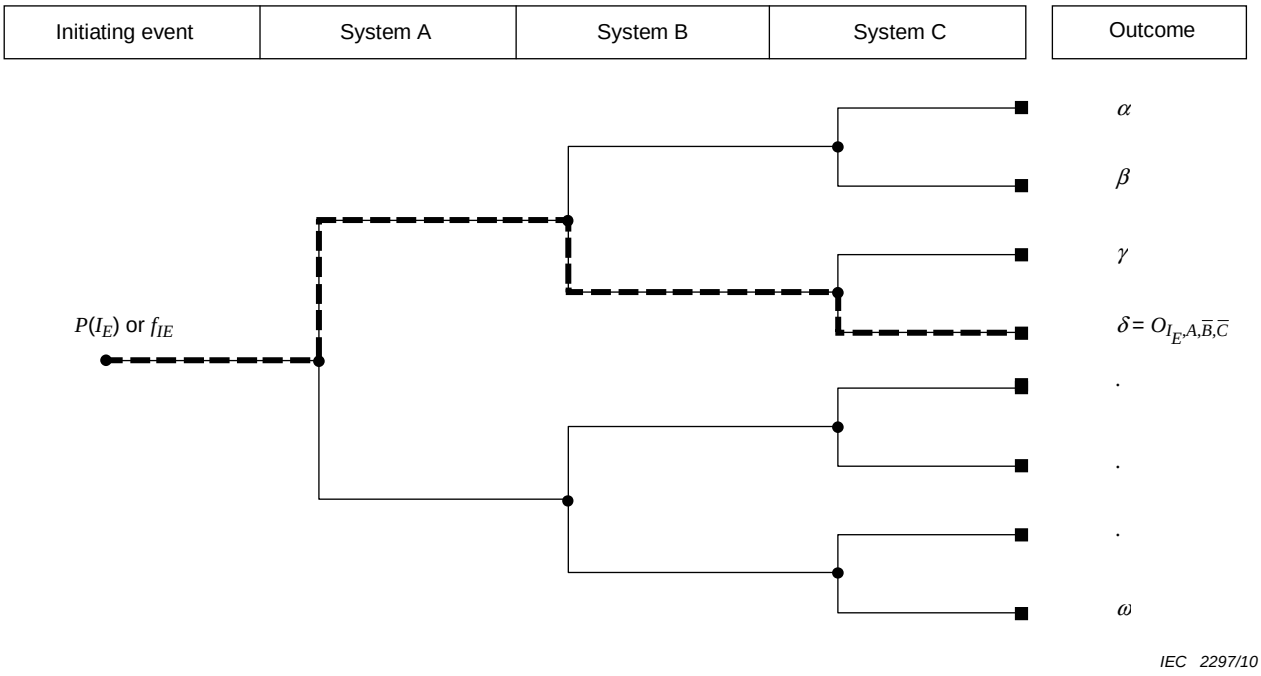

Figure 5 – Sequence of events

The conditional probability theorem together with the definitions in Clause 3 can be used to write down Equation (1) for the probability $P(\delta)$ of this particular sequence δ:

$$\begin{aligned} P(\delta) &= P\left(I_E \times A.\overline{B}.\overline{C}\right) \\ &= P(I_E) \times P(A \mid I_E) \times P\left(\overline{B} \mid I_E.A\right) \times P\left(\overline{C} \mid I_E.A.\overline{B}\right) \end{aligned} \quad (1)$$

where

$P(I_E)$ equals the probability of occurrence of the initiating event I_E,

$P(A \mid I_E)$ equals the probability of success of system A given the initiating event I_E has occurred (conditional probability).

If the successes and failures of one system are independent of those of the other systems, one can resort to probabilities conditioned solely on the occurrence if event I_E. Hence Equation (1) can be simplified as follows with $P(I_E)$ as the probability of occurrence of the initiating event:

$$P(\delta) = P(I_E) \times P(A \mid I_E) \times P(\overline{B} \mid I_E) \times P(\overline{C} \mid I_E) \quad (2)$$

The initiating event can be described either with a dimensionless probability of occurrence $P(I_E)$ or with a frequency f_{IE} (1/time). If the focus is on the concept of frequency, this mathematical model can also be used to calculate the frequency $f\delta$ of the sequence δ in Equation (3) with the frequency f_{IE} of the initiating event:

$$f_\delta = f_{IE} \times P(A \mid I_E) \times P(\overline{B} \mid I_E) \times P(\overline{C} \mid I_E) \quad (3)$$

Equation (3) has been used in the examples given in B.1.3, B.2.5, and B.2.6.

Conducting this evaluation for all possible sequences α, β, γ, δ,..., ω yields a complete quantification of the outcomes of the initiating event.

If the data for the occurrence of the initiating events is weak, it is recommendable not to rely completely on the quantification but rather to resort to sensitivity analysis in order to establish the most critical sequences.

8.3.2 Fault tree linking and boolean reduction

As pointed out in 6.1 and bearing in mind the limitations in 5.2, fault trees can be used to calculate the conditional probability for the failures of the mitigating factors.

Figure 6 displays an event tree with two mitigating factors, system A and system B. The probabilities of failure of systems A and B are denoted by $P(F_A)$ and $P(F_B)$ respectively, and are calculated by linking fault trees which, in this illustration only, are depicted with their top events as outputs from AND or OR gates according to IEC 61078 [16].

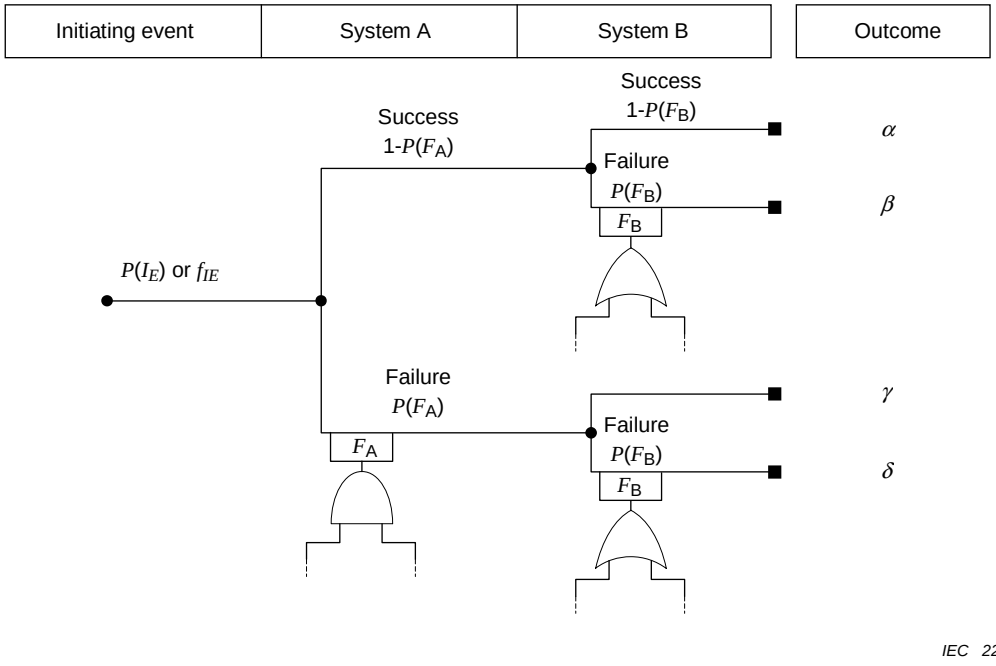

Figure 6 – Fault tree linking

The probabilities of the corresponding top events FA and F_B are used as the conditional probabilities $P(F_A)$ and $P(F_B)$ for the failure of system A and system B respectively. The

conditional probabilities for the successes of the systems are then given by 1 – $P(F_A)$ and 1 – $P(F_B)$.

When the mitigating factors are affected by common cause events, Boolean algebra may be used to reduce the event tree and identify these events.

The outcomes resulting from each event tree sequence is conducted using concepts given in [14]. The necessary Boolean reduction and prime implicant analysis is conducted according to [16].

Clause B.3 provides a detailed example of the Boolean reduction and prime implicant for a specific event tree.

In its original form, the top event of the fault tree linked to the various mitigating factors yields a probability of a specific state (e.g. success, failure) of the mitigating factor. These probabilities calculated by the FTA can be combined with the probability of occurrence or frequency of the initiating event (see 8.3.1). If the occurrence of the top event is expressed in terms of failure rates or frequencies, then these measures for the occurrence of the top event cannot be easily combined with the occurrence frequency of the initiating event. Hence one has to resort to other analysis techniques such as Markov modelling (see [17]). If non-trivial recovery or repair strategies for the various mitigating factors are involved, Markov modelling may facilitate a more realistic model. For a more detailed analysis of the different operation modes of a system and corresponding dependability measures, one can refer to [18].

Further details about the mathematical foundations of event tree calculation can be found in [32].

The basic rules for quantification relatively straightforwardly lend themselves to being implemented on a computer. Many software packages are available to facilitate the qualitative and quantitative analysis of an event tree. However, it is IEC policy not to recommend a specific software package.

Practical examples illustrating the theoretical considerations in this clause are given in Annex B.

Besides the more theoretical aspects of reordering, extraction and fault-tree Boolean operations, it is important to set clear guidelines for both the objectives and the requirements for the analysis. A more comprehensive approach to establishing a concise procedure for ETA is provided in [3].

9 Documentation

The documentation of ETA should include some basic items as listed below. Additional and supplementary information may be provided to increase clarity, especially for complex systems. The key point is that the documentation must comprehensively capture the performed steps.

In the following, the clauses in brackets refer to an example in Clause B.2:

a) objective and scope of the analysis (B.2.2), (B.2.4);

b) system description (B.2.3):

   1) design description;

   2) system operation;

   3) detailed system boundaries definitions.

c) assumptions (B.2.3), (B.2.4):

1) system design assumptions;
2) operation, maintenance, test and inspection assumptions;
3) reliability and availability modelling assumptions.

d) ETA (B.2.5), (B.2.6):
1) rationale and sources for the list of initiating events;
2) analysis, including the graphical representation;
3) sources of data used.

e) results, conclusions and recommendations (B.2.7).

For more general guidance on documentation, see [13].

Annex A
(informative)

Graphical representation

A frequently used graphical representation for an event tree is given in Figure A.1:

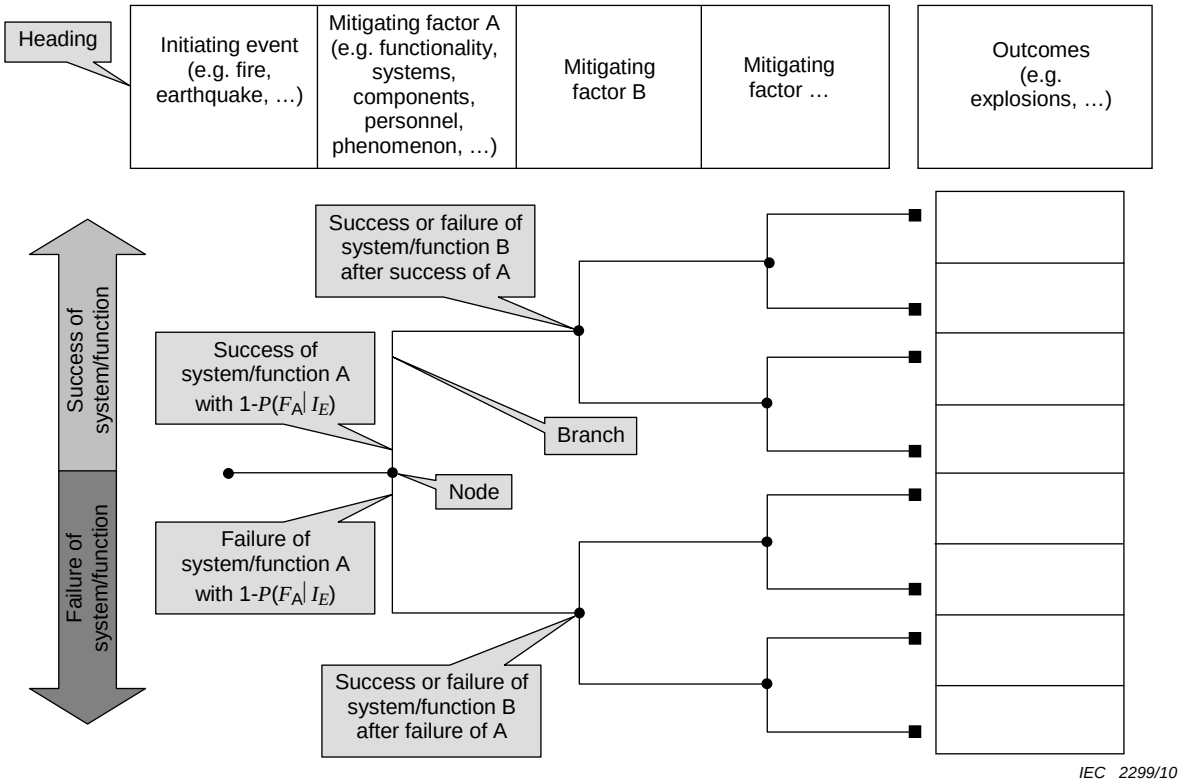

Figure A.1 – Frequently used graphical representation for event trees

The explanations of the graphical elements are provided in Table A.1:

Table A.1 – Graphical elements

Element	Remarks
Branch	See 3.1.10 – Note that there may be two or more branches originating from a node, for details see also 7.2.5 c)1). It has to be noted, that only in the case of binary branches do the Boolean methods in Clause B.3 apply
Heading	See 3.1.4
Initiating event	See 3.1.5
Mitigating factor	See 3.1.6
Node	See 3.1.1
Outcome	See 3.1.7
$P(F_A\|I_E)$	Probability of the failure of mitigating factor A under the condition that the initiating event (I_E) has occurred
Success/failure	In order to map unambiguously the possible outcomes to the success or failure of the system or function, it is imperative to establish clear-cut criteria for success and failure, respectively

Annex B
(informative)

Examples

B.1 Fire incident in a nuclear power plant

B.1.1 Overview

Experience over the last 40 years has shown that risks from fire in a nuclear power plant should be taken into account when analysing the contributing factors for the overall risk of a severe nuclear accident.

The following is a probabilistic fire risk analysis performed with a twofold objective:

a) the critical plant zones that present the largest contribution to the total core damage probability of the nuclear power plant shall be identified by an appropriate screening process;

b) fire event sequences shall be established which reflect the effects of fire occurrence, fire detection, room isolation, fire suppression and equipment damage due to the suppression agent.

In a quantitative ETA, the frequency of initiating events caused by fire and different core damage states shall be determined.

The major tasks are the quantitative analysis and the qualitative screening process to identify critical fire compartments, as described below.

B.1.2 Screening analysis

In the first step, a detailed data collection is done in all rooms of the plant to classify them according to their importance and function. The following terms are examples from a specific analysis.

A fire area is defined as a building or part of a building, sufficiently protected by fire barriers which prevent fire propagation to adjacent buildings or parts of buildings.

A fire compartment is a subdivision of a fire area so that undesired consequences do not spread to other subdivisions.

An essential fire compartment contains either equipment related to power operation, safety related equipment or fixed or temporarily located combustibles.

A critical fire compartment is that essential fire compartment in which if a fire damages at least one safety-related component or system, it causes a safety related initiating event in the nuclear power plant.

The screening process starts with the identification of all rooms for which at least one of the following three criteria is fulfilled:

a) fire load >7 kWh/m^2;

b) room contains safety-related equipment or cables of such equipment;

c) room contains operational or sensing equipment of the reactor protection system (safety control system).

Rooms for which all three criteria are fulfilled simultaneously will be identified as essential fire compartments.

B.1.3 Quantitative analysis

For each critical fire compartment, an event tree will be developed with node for fire initiation, ventilation of the room, fire detection, fire suppression and propagation. All mitigating factors in the event tree are considered as independent of each other (see limitations in 5.2). Figure B.1 shows a typical event tree for an oil fire in a diesel generator room.

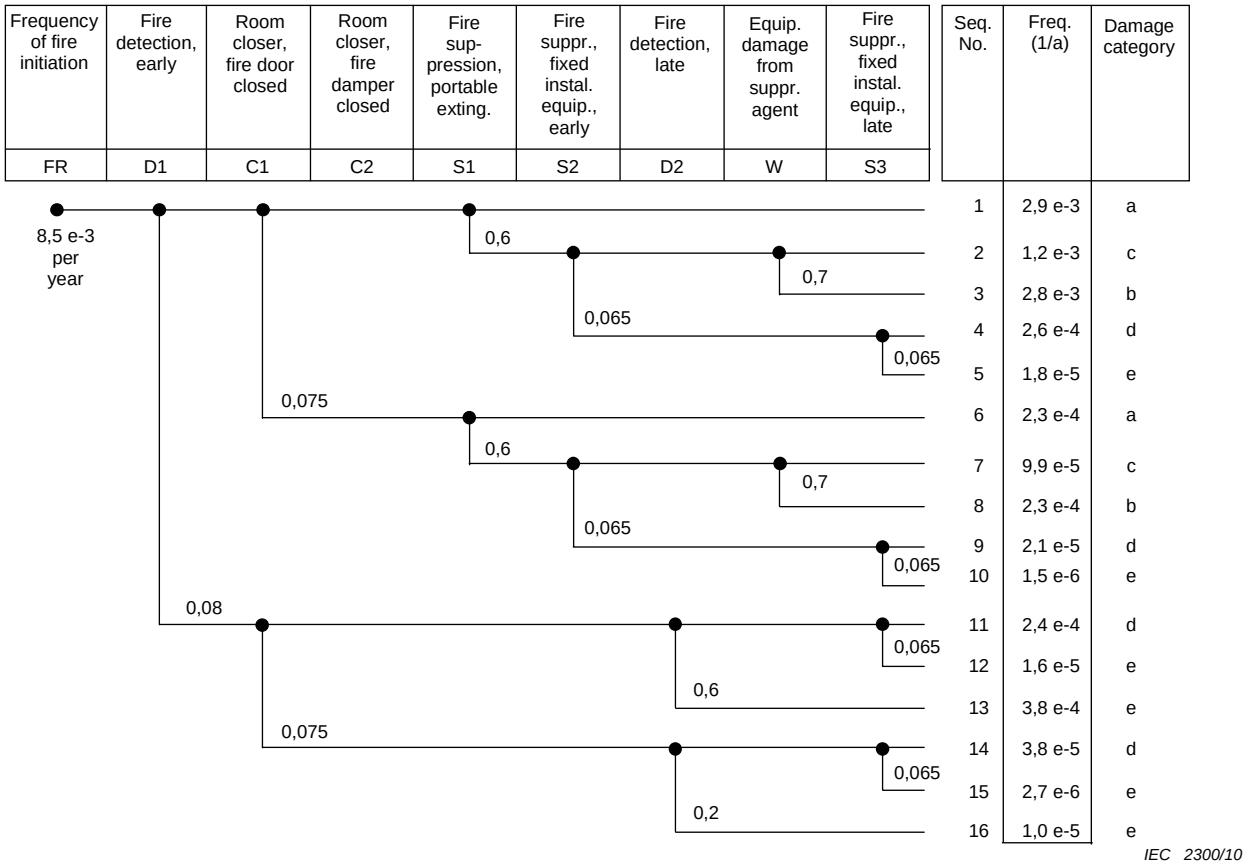

Figure B.1 – Event tree for a typical fire incident in a diesel generator building

For the fire ignition frequency and the different nodes, appropriate data shall be used. Such data should, as far as possible, be plant specific. However, in case of lack of plant specific data, publicly available international data bases such as the latest published data base for US plants can be used. To calculate the fire frequency for a single room in a building, additional weighting factors based on the amount of ignition sources, the weight of cable insulation, the number of relevant fire zones and special factors for the ignition sources are required.

The outcomes are distinguished in five damage categories (a), (b), (c), (d) and (e). The worst category is defined as (e) “Total damage and propagation”, which occurs when all fire protection measures fail to prevent the propagation to adjacent rooms. All safety-related equipment is damaged in the neighbouring rooms.

For each critical fire compartment, the following results are obtained:

a) frequency and nature of fire initiated transients in the nuclear power plant;

b) a list of damaged equipment, categorized according to the damage category (a) – (e);

c) frequency of the damage categories.

Figure B.2 provides a simplified version of an event tree. The frequency of a flashover fire initiated by an incipient fire and the subsequent unavailability of the fire detection is derived by multiplying the frequency of the initiating event of 1,0e-4 per year by the probability of the unavailability of the fire detection of 1,0e-3 per year. This yields a resulting frequency of 1,0e-7 per year of the undesired event of a flashover fire.

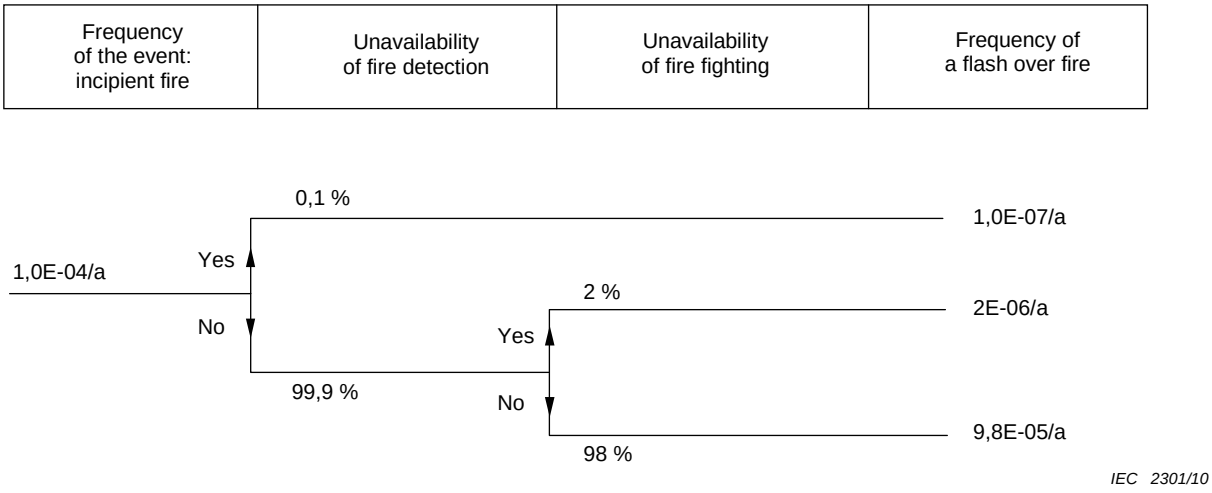

Figure B.2 – Simplified event tree for a fire event

B.1.4 Results

ETA provides an excellent tool to catalogue, evaluate and discuss possible deficiencies and to set priorities for fire protection improvement measures. Additional cost/benefit studies can be based on the results.

B.2 ETA for a level-crossing system

B.2.1 Symbols and acronyms

Symbols used in this annex are given below in Table B.1.

Table B.1 – Symbols used in Annex B

Symbol	Description
A_k	Accident scenario, k
C_k	Outcome probability
D	Hazard duration
E	Total exposure per usage
F_k	Probability of fatality
IRF	Individual risk of fatality
H	Hazard
HR	Hazard rate (in the sense of “instantaneous failure rate”, see 6.1.3 of IEC 61703:2001 [20])
k	Numbering for the different scenarios
LX	Level crossing
N	Number of times the level crossing is used per year by a person
THR	Tolerable hazard rate (in the sense of “instantaneous failure rate”, see 6.1.3 of IEC 61703:2001[20])

Symbol	Description
P_C	Probability of “collision with train”
P_{EA}	Probability of “unable to take evasive action”
P_N	Probability of “no timely notice of train”
P_{Tr}	Probability of “train is approaching”
TIR	Target for the Individual acceptable level of the Risk

B.2.2 Objective

So as to illustrate the application of ETA, Clause B.2 provides an example of a risk-orientated apportionment of safety integrity requirements for a system from the railway signalling sector, a level crossing.

The objective of the analysis is to derive safety targets for a defined initiating event, taking into account all operational, environmental and architectural conditions. This objective is attained by means of a “reversed” ETA (see B.2.6). “Reversed” event tree in this context means to derive the tolerable frequency for the initiating event by inverting the way of calculation starting from the outcomes.

Neither the functionality nor the analysis bears any direct resemblance to the features of a particular type of level crossing. The major aim is to present an example of the methodology, rather than provide a detailed realistic analysis. In particular, the values used in the calculations are examples and should not to be regarded as factual.

B.2.3 System definition

The following example from a railway signalling sector of an automatic level crossing, has been the subject of many analyses for illustration purposes.

In this example, the automatic level crossing has been in operation for a period of 25 years and uses light signals to warn the road user and a distant (monitoring) signal to tell the train driver whether the level crossing is closed or not.

A diagram of the level crossing (LX) is given in Figure B.3.

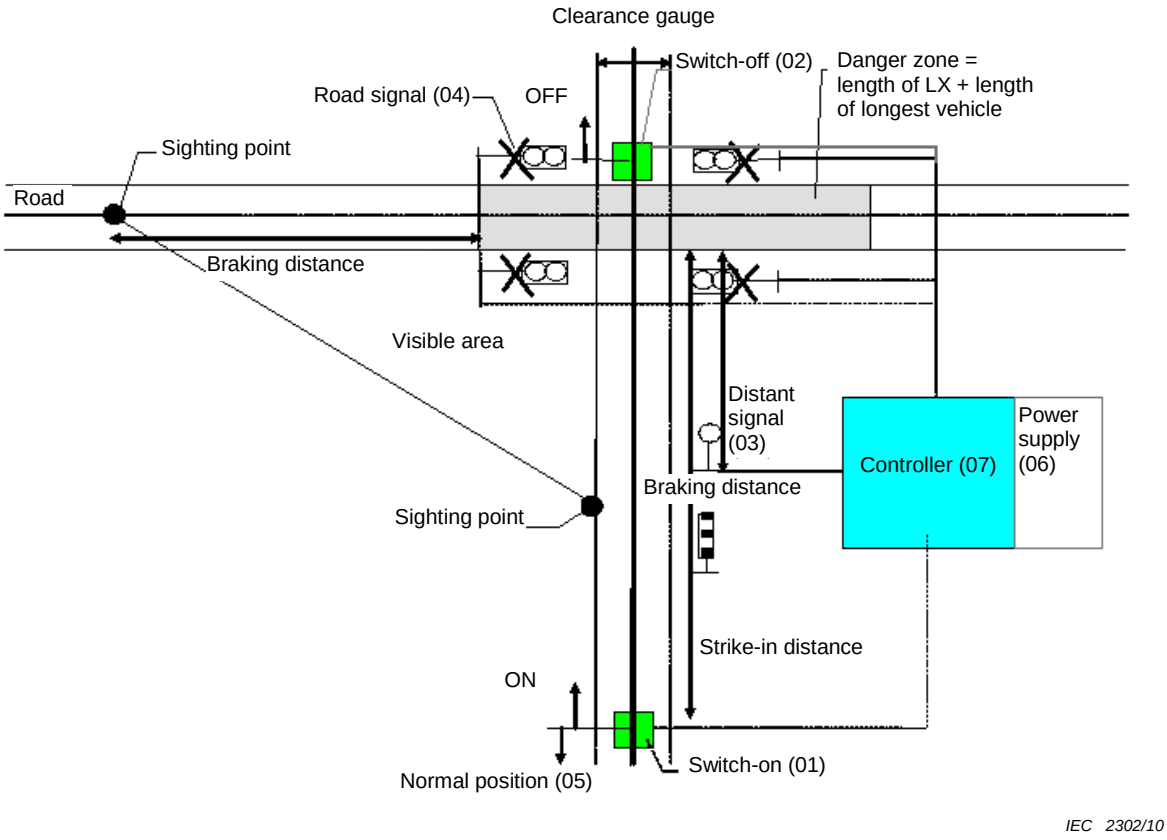

Figure B.3 – Level-crossing system (LX)

As a full system definition is beyond the scope of this example, only an informal functional description is given here. Table B.2 provides an overview of the principal functional units involved.

Table B.2 – System overview

No.	Functional unit	Remarks
01	LX switch-on	Triggers activation of the LX when a train approaches (implemented by means of wheel detection equipment, e.g. an axle counter)
02	LX switch-off	Triggers deactivation of the LX once a train has left the crossing (implemented by means of wheel detection equipment, e.g. an axle counter)
03	LX monitoring	Displays the state of the LX to the train driver or interlocking (implemented e.g. by means of a distant signal) to allow monitoring of LX operation
04	Road signalling	Displays the state of the LX to road users
05	Normal position	Returns the LX to the normal position (no protection) if it is switched on and then not switched off within a certain time (due, e.g. to a detector failure which continues to signal a train even when it has already passed the LX or when the train has stopped before the LX, etc.)
06	Power supply	Consists of the normal power supply system or, as a fall-back level, a battery capable of operating the LX for a limited period, e.g. 2 h. The battery voltage is monitored by the interlocking
07	Control	Operates and controls the LX. A programmable electronic device which contains application software, site-specific data, etc.

A brief description of fault-free operation of the level crossing is given as follows:

a) An approaching train is detected by the switch-on element (01) and indicated to the controller (07). The distance of the switch-on element (01) from the level-crossing is denoted as the “strike-in distance”.

b) The controller issues the command to activate the road signals (04) and waits until an indication of successful switch-on has been received. The distance between the sighting point and the level crossing is denoted as the “braking distance”.

c) The controller issues the command to activate the distant signal (03), depicted by a small circle on a small vertical line perpendicular on a small horizontal line. The default position is off (danger). When the distant signal is off, an approaching train must stop at the level crossing and the driver may then switch on the level crossing manually using a key as the fall-back mode.

d) Traversal of the level crossing by the train is detected by a switch-off element (02) and indicated to the controller.

e) The controller issues the command to switch off the distant signal. After a delay, the road signals are switched off.

B.2.4 Hazard identification

In the railway sector, the initiating events at the system level are labelled as hazards according to the relevant CENELEC standards.

A complete analysis of the possible hazards is not performed; instead only the hazard H as stated below is considered.

H = Failure of level crossing to protect public from train

It is interpreted as covering all situations in which the level crossing should warn the public (of approaching trains), but fails to do so.

The objective is to determine the hazard rate HR (1/time) for H which is acceptable according to certain risk acceptance criteria. “Rate” is used in the sense of “instantaneous failure rate”, as described in 6.1.3 of IEC 61703:2001 [20].

B.2.5 ETA

In order to determine the possible outcomes of the hazard H, one has to look at a scenario in which an individual encounters H. Hence as an example, one particular case of a motorist approaching an unprotected level crossing is considered, with P_{TR} denoting the probability of no train approaching, P_N the probability of timely notice of the train by the driver, P_{EA} the probability of an evasive action, and P_C the probability of an actual collision with the train.

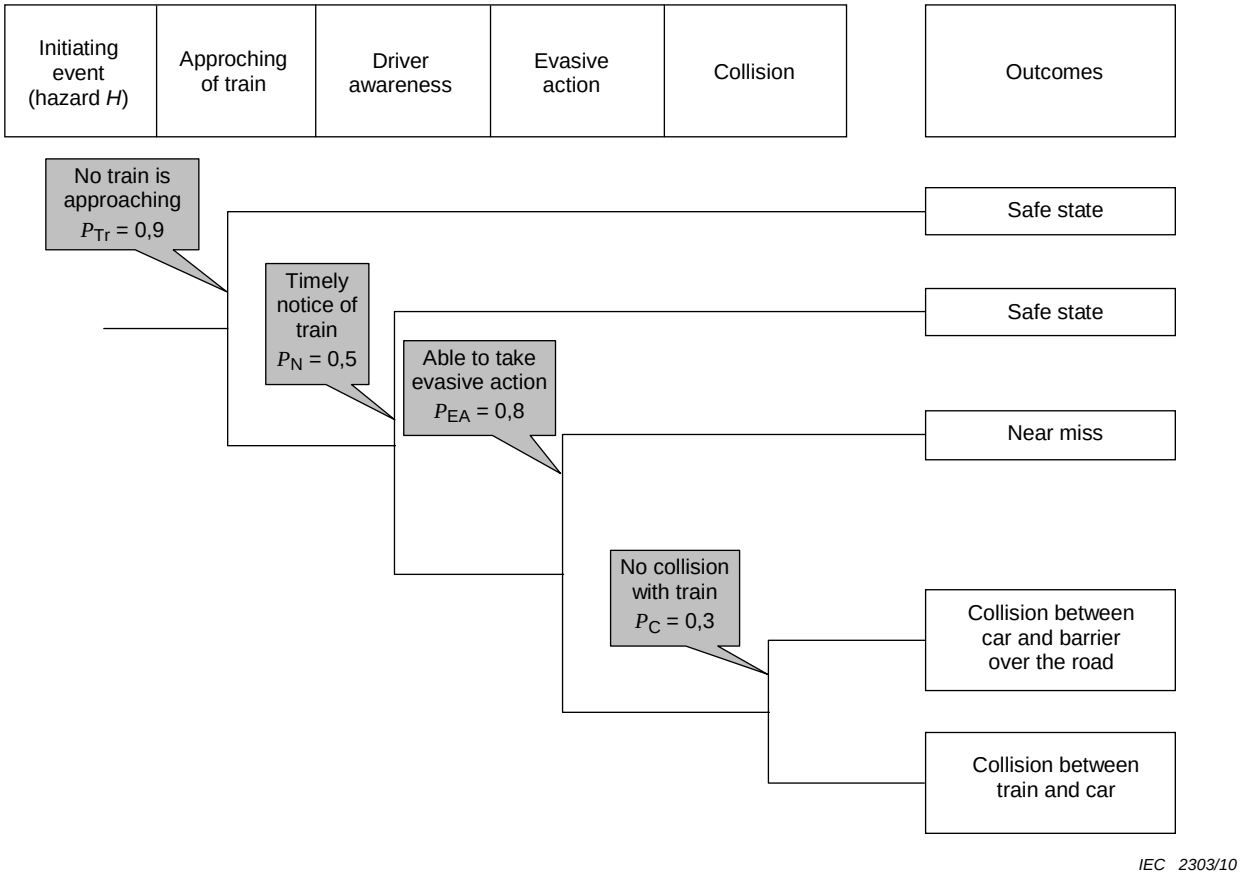

Figure B.4 – ETA for a level-crossing system

Thus two types of accidents ("Collision between train and car" and "Collision between car and level crossing") are identified. Figure B.4 shows the external risk reduction factors (i.e. mitigating factors, see 3.1.6) between the initiating event, i.e. the hazard, and the outcomes, i.e. the accidents.

B.2.6 Quantitative analysis

NOTE Bearing in mind the limitations given in 5.2, the following quantitative analysis concerns itself with conservative results.

The benchmark figures of Railtrack's Railway Group Safety Plan (1997/98) [33] are taken as the targets for the individual acceptable level of the risk (TIR) for an individual motorist: "Reasonably practicable schemes will continue to be implemented with the aim of ensuring that automated level crossings expose the individual occupants of road vehicles to a risk of fatality no greater than one in 100 000 regular users per annum by the year 2 000".

In order to define a broadly acceptable limit, an additional safety factor of 10 is added. This means that the individual risk derived from R_i <10^{-5} fatalities/(person × year) for a regular user should be less than 10^{-6} per year. Thus the TIR value is established at less than 10^{-6} per year.

In order to obtain the approval from the authorities, the railway undertaking has to prove that the actual Individual Risk of Fatality (IRF) is less or equal to TIR. The following derivation of the acceptable rate for the hazard is based on the equation for IRF from [4]. This mathematical model for the determination of individual risk takes account of the causality leading from the initiating event, i.e. the hazards, to the outcomes, or accident sequences.

a) It is assumed that an individual uses the level crossing with a usage profile, which is described by the number of times it is used N (per year). For reference, a total exposure per usage E may be defined (i.e. E is the time needed to traverse a level crossing).

b) In this example, the individual is exposed to hazard H. The probability that the individual will be exposed to the hazard depends additionally on the hazard duration D and the exposure time E of the individual to the hazards. This probability consists of the sum of the probabilities that the hazard already exists when the individual enters the system (approximately HR x D) and the probability that the hazard will occur while the individual is exposed (approximately HR x E).

c) From each hazard one or more types of accident sequences may result. This is described for each hazard by the outcome probability C_k that an accident A_k will occur. This probability stands for the external risk reduction factors (i.e. mitigating factors, see 3.1.6) obtained by ETA (Figure B.4). For each associated type of accident A_k, there is a corresponding severity. At the individual level, this is described as the probability of a fatal accident, F_k for a single individual (Table B.3).For the sake of the example, the accident severity was estimated and compared with the railtrack data [33].

Table B.3 – Risk reduction parameters for accidents from Figure B.4

No. k	Accident A_k	Risk reduction factor C_k	Probability of fatality F_k
1	Collision between train and car	0,1×0,5×0,2×0,7 = 0,007	0,2
2	Collision between car and a level crossing	0,1×0,5×0,2×0,3 = 0,003	0,05

This gives rise to an individual risk of fatality defined by

$$\mathrm{IRF} = \mathrm{N} \times H_{\mathrm{R}} \times (D + E) \times \sum_{\text{accidents } A_k} (C_k \times F_k) \tag{B.1}$$

Equation (B.1) can be evaluated either by using mean values or by inserting appropriate parameters (e.g. percentiles) of statistical distributions for the input parameters.

If the individual risk turns out to be less than the target individual risk, the calculated or estimated hazard rate (HR) is called tolerable hazard rate (THR).

For the purpose of this example, a motorist is considered to cross a railway line repeatedly, say N = 1 000 times a year. Other users such as pedestrians or cyclists are not taken into account.

Based on operational experience, it is assumed that the hazard H, if it occurs, lasts much longer than the individual exposure time, which would be the time to cross the level crossing. This means we can ignore the individual exposure time E in Equation (B.1). As a pessimistic value, a hazard duration time of D = 10 h is assumed, which is the time of a failure of the LX, which results in a dangerous state of the system, lasts (until negated or repaired).

The tolerable hazard rate (THR) for H can be calculated by inserting the parameters in Equation (B.2) as follows:

$$\begin{aligned} \mathrm{IRF} &= \mathrm{N} \times H_{\mathrm{R}} \times (D + E) \times \sum_{\text{accidents } A_k} (C_k \times F_k) \\ &= 1\ 000 \times \mathrm{H}_{\mathrm{R}} \times 10 \times (0{,}007 \times 0{,}2 + 0{,}003 \times 0{,}05) \\ &\leq \mathrm{TIR} = 10^{-6} \text{ per year} \end{aligned} \tag{B.2}$$

This yields a tolerable rate for the occurrence of the initiating event, i.e. the hazard, of approximately 7×10^{-8} h^{-1}, corresponding approximately to one tolerable failure of the level crossing to protect public from train per 1 600 years.

B.2.7 Analysis of the outcomes and definition of necessary action

On completion of the analysis, it is the task of the designer or manufacturer of the level crossing to investigate whether the tolerable hazard rate can be achieved by his system or if architectural or design changes need to be made so as to meet the quantitative targets.

B.2.8 Conclusion

This railway signalling example has shown an alternative approach to ETA, whereby one uses a reverse approach deriving tolerable rates for the initiating event from the observed outcomes using risk reduction parameters.

B.3 Fault tree linking and boolean reduction

NOTE This clause provides the theoretical concepts behind the most often used software packages for Boolean reduction. The reader should comprehend the basic algorithms so as to gain a profound understanding of the technique. This approach is applicable to event trees with binary branches only.

When different mitigating factors share a common cause factor, Boolean algebra may be used to identify these common causes during the qualitative evaluation of the event tree. The prime implicants resulting from the qualitative analysis are then used in the quantification of the frequency of a specific outcome.

Indeed, each outcome is obtained by combining, through an AND logic gate, the top events of the linked fault trees (see 8.3.2) related to the failure of the mitigating factors. Likewise, the “prime implicants” of this new logic tree are sought.

Minimal sequences are the smallest combination of events resulting in unacceptable outcomes. Minimal sequences are, in fact, a special instance of “prime implicants”. When the fault tree is coherent (contains only AND gates and OR gates), the phrase “prime implicants” can thus be replaced by “minimal sequences”. For more details on the theory of “prime implicants” and minimal sequences, see [38].

The “prime implicants” are identified for the event resulting from an AND-gate combination of events only related to the failures of mitigating factors. An example of Boolean reduction of an event tree is presented in Figure B.5.

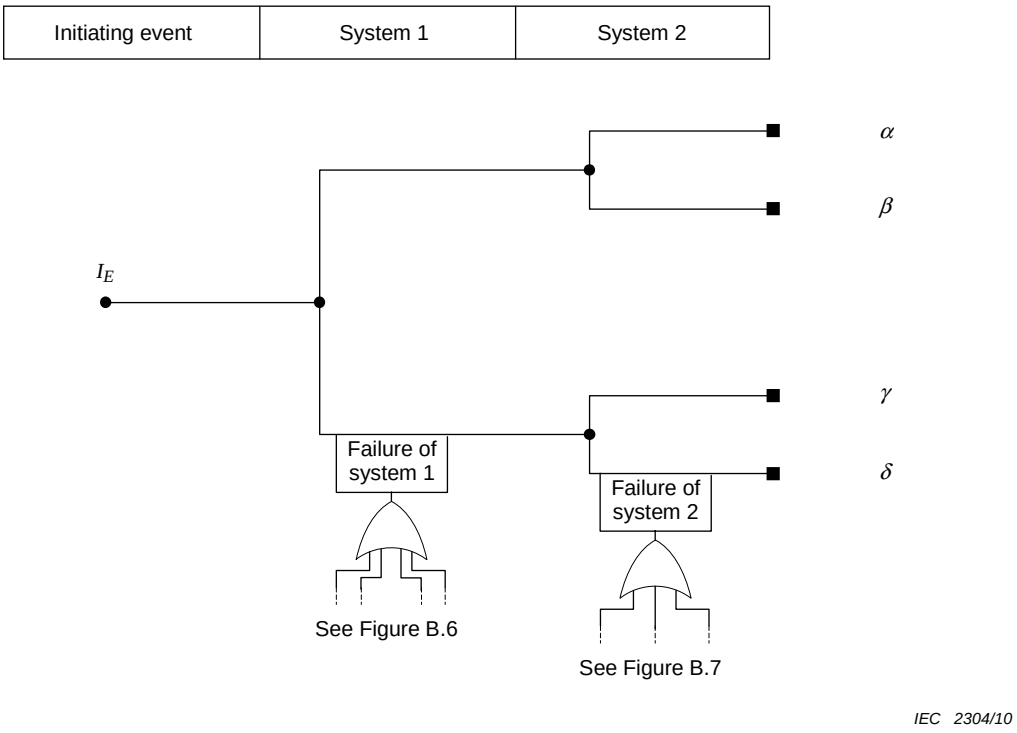

Figure B.5 – Simple example

The probabilities for the failures of system 1 and system 2 can be modelled by fault tree linking as described in 8.3.2.

The following theoretical fault trees represent the logical structure respectively for the failure of system 1 (see Figure B.6) and system 2 (see Figure B.7) involving seven basic events A, B, C, D, E, F, and G. The symbols are used in accordance with IEC 61078 [16].

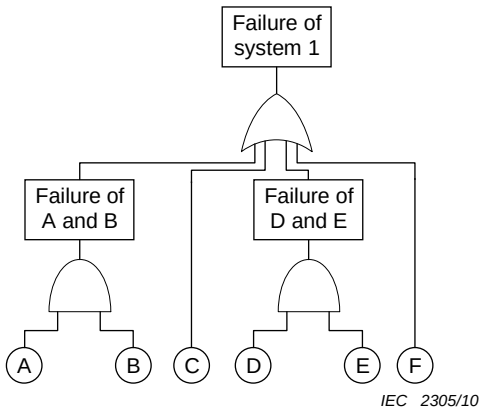

Figure B.6 – Fault tree for the failure of system 1

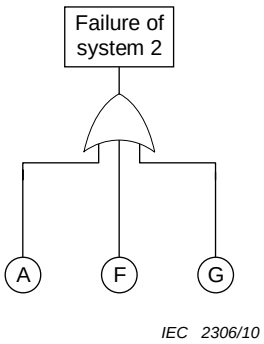

Figure B.7 – Fault tree for the failure of system 2

Together with these fault trees and the event tree, the reduced Boolean expressions for the outcomes α, β, γ, δ are as follows:

$$\alpha = I_E.\left(\overline{A}.\overline{C}.\overline{D}.\overline{F}.\overline{G} + \overline{A}.\overline{C}.\overline{E}.\overline{F}.\overline{G}\right) \quad \text{(B.3)}$$

$$\begin{aligned}\beta = I_E.(&A.\overline{B}.\overline{C}.\overline{D}.\overline{F} + A.\overline{B}.\overline{C}.\overline{E}.\overline{F} + \\ &+ \overline{A}.\overline{C}.\overline{D}.\overline{F}.G + \overline{A}.\overline{C}.\overline{E}.\overline{F}.G + \\ &+ \overline{B}.\overline{C}.\overline{D}.\overline{F}.G + \overline{B}.\overline{C}.\overline{E}.\overline{F}.G)\end{aligned} \quad \text{(B.4)}$$

$$\gamma = I_E.\left(\overline{A}.C.\overline{F}.\overline{G} + \overline{A}.D.E.\overline{F}.\overline{G}\right) \quad \text{(B.5)}$$

$$\delta = I_E.\left(F + A.B + A.C + G.C + A.D.E + G.D.E\right) \quad \text{(B.6)}$$

If δ is the outcome to be analysed, the prime implicants are

$$I_E.F, \quad I_E.A.B, \quad I_E.A.C, \quad I_E.G.C, \quad I_E.A.D.E, \quad I_E.G.D.E$$

The basic events A and F are common to both fault trees. According to 8.2.3, they may be extracted – to yield System 1* (S_1^*) and System 2* (S_2^*) without A and F – and introduced as new mitigating factors into a new event tree (see Figure B.8).

Note that in this particular instance A and F being used in a fault tree environment denotes the occurrence of failure events leading to a failure of the systems (Figure B.6 and Figure B.7). Thus the upper branch denotes a development towards the failure of the system.

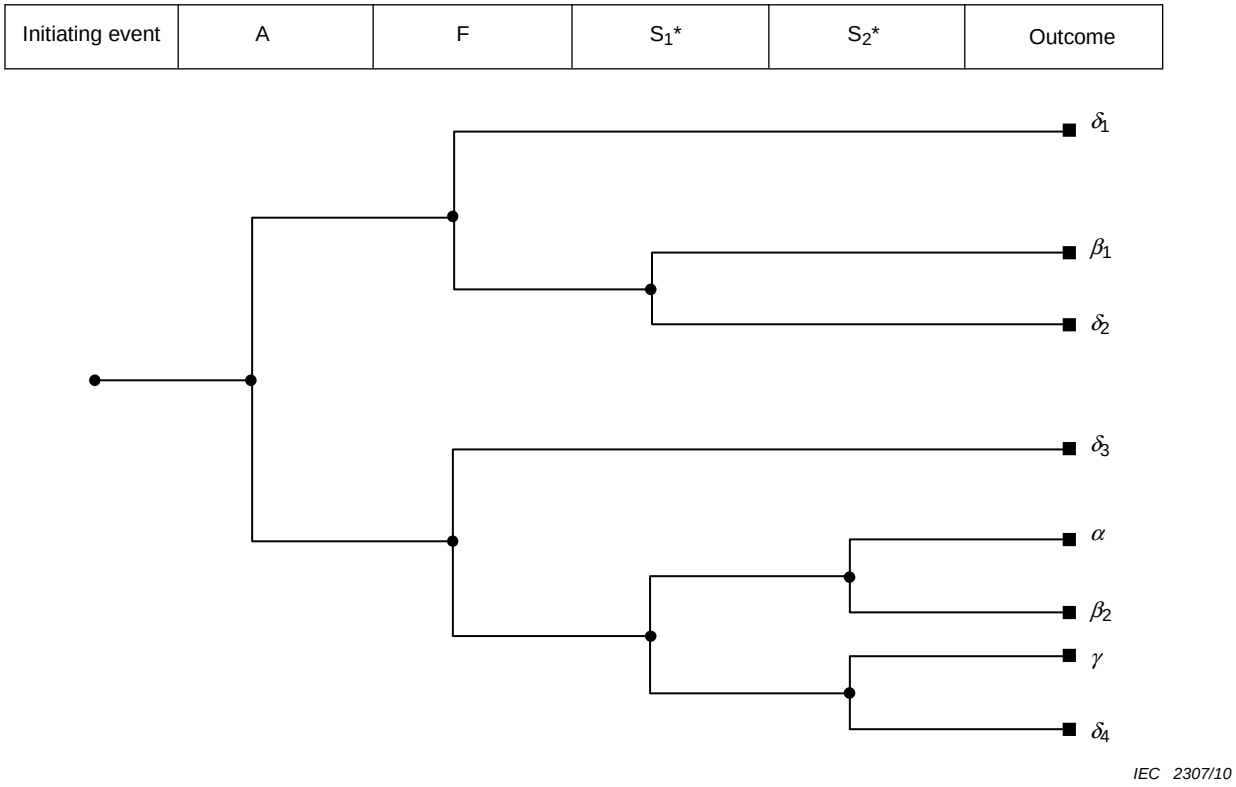

Figure B.8 – Modified event tree

The equivalence between these two schematics and the following equalities can be verified (see [16]):

$$\beta = \beta_1 + \beta_2 \tag{B.3}$$

as well as

$$\delta = \delta_1 + \delta_2 + \delta_3 + \delta_4 \tag{B.4}$$

with

$$\beta_1 = I_E.\left(A.\overline{F}\,.\,S_1^*\right),$$

$$\beta_2 = I_E.\left(\overline{A}.\overline{F}\,.\,S_1^*.\,\overline{S}_2^*\right),$$

$$\delta_1 = I_E.\left(A.\,F\right),$$

$$\delta_2 = I_E.\left(A.\,\overline{F}\,.\,\overline{S}_1^*\right),$$

$$\delta_3 = I_E.\left(\overline{A}\,.\,F\right), \text{ and}$$

$$\delta_4 = I_E.\left(\overline{A}.\,\overline{F}\,.\,\overline{S}_1^*.\,\overline{S}_2^*\right).$$

The following “global grouped faults” can be examined:

“Loss of system 1”:

$$G_1 = D.E + C \tag{B.5}$$

“Loss of system 2”:

$$G_2 = A + G \tag{B.6}$$

“Loss of systems 1 and 2”:

$$G_3 = F + A.B \tag{B.7}$$

The event tree assumes the following form:

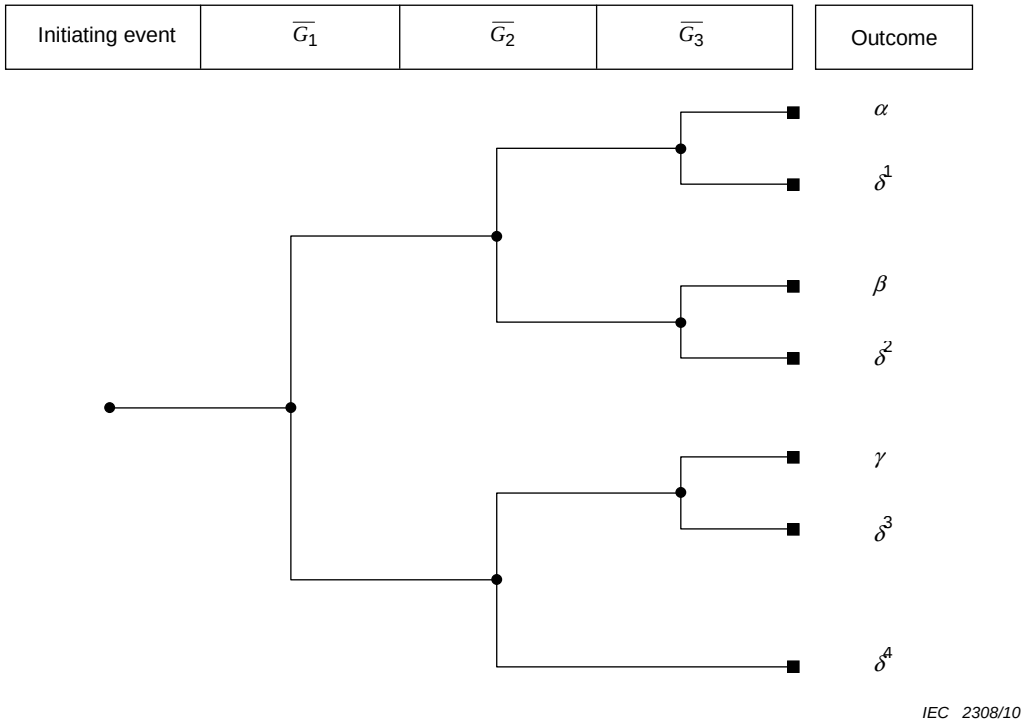

Figure B.9 – Event tree with "grouped faults"

The equivalence between these schematics and the following equality can be verified (see IEC 61078 [16]):

$$\delta = \delta^1 + \delta^2 + \delta^3 + \delta^4 \tag{B.8}$$

with

$$\delta^1 = \overline{G_1} \,.\, \overline{G_2} \,.\, G_3 \,,$$

$$\delta^2 = \overline{G_1} \,.\, G_2 \,.\, G_3 ,$$

$$\delta^3 = G_1 \,.\, \overline{G_2} \,.\, G_3 \text{, and}$$

$$\delta^4 = G_1 \,.\, G_2 \ .$$

A more thorough approach to Boolean analysis, including detailed advice on disjointing methods, can be found in IEC 61078 [16].

Bibliography

[1] American Institute of Chemical Engineers, *Layer of Protection Analysis – Simplified process risk assessment*, New York, USA, October 2001

[2] ANDREWS, J.D., DUNNETT, S.J. *Event Tree Analysis using Binary Decision Diagrams*, IEEE Trans. Reliability, Vol 49, pp 230 – 238, 2000

[3] ASME Standard for *Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME RA-S-2002, 2002, Amended by addenda ASME RA-Sa-2003, ASME RA-Sb 2005, and ASME RA-Sc-2007

[4] BRABAND, J., LENNARTZ, K. *A Systematic Process for the Definition of Safety Targets for Railway Signalling Applications*, Signal+Draht, 9/99

[5] DOWELL, III, A.M., HENDERSHOT, D.C. *Simplified Risk Analysis – Layer of Protection Analysis (LOPA)*, American Institute of Chemical Engineers, Indianapolis, 2002

[6] Expert Group on Probabilistic Safety Analysis for Nuclear Power Plants: "*Methods for Probabilistic Safety Analysis for Nuclear Power Plants, Status: August 2005*", BfS-SCHR-37/05, Salzgitter, October 2005 (In German)

[7] FULLWOOD, R.; HALL, R. *Probabilistic Risk Assessment in the Nuclear Power Industry*, New York, 1988

[8] GOLDBERG, B.E., EVERHART, K., STEVENS, R., BABBITT III, N., CLEMENS,P., STOUT, L. *System Engineering "Toolbox" for Design-Oriented Engineers*, NASA Reference Publication 1358, 1994

[9] *Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, NRC 1998.

[10] HENLEY, E.J., KUMAMOTO, H. *Reliability Engineering and Risk Assessment*, 1981

[11] HOFER, E., KLOOS, M., KRZYKACZ-HAUSMANN, B., PESCHKE, J., SONNENKALB, M. *Dynamic Event Trees for Probabilistic Safety Analysis, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS)*, Proceedings EUROSAFE, Berlin 4-5 November 2002

[12] ISO/IEC 31010, *Risk management – Risk assessment guidelines*

[13] IEC 60300-3-1:2003, *Dependability Management – Part 3-1: Application guide – Analysis techniques for dependability - Guide on methodology*

[14] IEC 60300-3-9:1995, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

[15] IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

[16] IEC 61078:2006, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

[17] IEC 61165:2006, *Application of Markov techniques*

[18] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[19] IEC 61511-3:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

[20] IEC 61703:2001, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

[21] IEC 62425:2007, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

[22] IEC 62429:2007, *Reliability growth – Stress testing for early failures in unique complex systems*

[23] IEC 62508:2010, *Guidance on human aspects of dependability*

[24] IEC 62551, *Analysis techniques for dependability – Petri net techniques*[2]

[25] ISO 3534-1:2006, *Statistics – Vocabulary and symbols – Part 1: General statistical terms and terms used in probability*

[26] KLOOS, M., PESCHKE, J., MCDET: *A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach, Nuclear Science and Engineering*: 153, 137-156, 2006

[27] LEVESON, N.G. SAFEWARE: *System Safety and Computers*, Addison-Wesley Publishing Company, 1995

[28] McCORMICK, N.J. *Reliability and Risk Analysis – Methods and Nuclear Power Applications*, Boston, 1981

[29] Nuclear Regulatory Commission, PRA Procedures Guide, *A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, Final Report, NUREG/CR-2300 Vol. 1, January 1983

[30] NIELSEN, D.S. *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*, Danish Atomic Energy Commission, RISO-M-1374, May 1971

[31] Nuclear Regulatory Commission, Reactor Safety Study: *An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, Rep. WASH-1400-MR (NUREG-75/014), Washington, DC, 1975

[32] PAPAZOGLOU, I. A. *Mathematical foundations of event trees, Reliability Engineering and System Safety 61* (2008) 169-183, Northern Island, 2008

[33] *Railtrack, Engineering Safety Management System*, Issue 2.0, "Yellow Book", 1997

[34] RAUSAND, M., HOYLAND, A. *System Reliability Theory – Models, Statistical Methods and Applications*, Hoboken, New Jersey, 2004

[35] SIU, N. *Risk Assessment for Dynamic Systems:* An Overview, Reliability Engineering and System Safety 43, 1994, p. 43-73

[36] SMITH, D.J. *Reliability, Maintainability and Risk*, Oxford, 2001

_____

2 Under consideration, see 56/1322/CD.

[37] Special subject: *Common cause failure analysis*, Kerntechnik Vol 71, No 1-2, Carl Hanser-Verlag, February 2006, pp 8 – 62

[38] VILLEMEUR, A. *Reliability, Availability, Maintainability and Safety Assessment*. Volume 1. Methods and Techniques, Chichester, Wiley, 1992

[39] XU, H.; DUGAN, J.B. *Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment*, University of Virginia, January 2004

[40] ZIO, E. *An Introduction to the Basics of Reliability and Risk Analysis*, Series in Quality, Reliability and Engineering Statistics, Vol. 13, 2007

_____

SOMMAIRE

AVANT-PROPOS 46
INTRODUCTION 48
1 Domaine d'application 49
2 Références normatives 49
3 Termes, définitions, abréviations et symboles 49
3.1 Termes et définitions 49
3.2 Abréviations et symboles 51
3.2.1 Abréviations 51
3.2.2 Symboles 51
4 Description générale 52
5 Avantages et limites de l'AAE 53
5.1 Avantages 53
5.2 Limites 53
6 Relation avec d'autres techniques d'analyse 54
6.1 Combinaison de l'AAE et de l'AAP 54
6.2 Analyse des niveaux de protection (LOPA) 56
6.3 Combinaison avec d'autres techniques 56
7 Développement des arbres d'événement 56
7.1 Généralités 56
7.2 Étapes de l'analyse par arbre d'événement 57
7.2.1 Mode opératoire 57
7.2.2 Étape 1: Définition du système ou de l'activité considéré(e) 57
7.2.3 Étape 2: Identification des événements initiateurs considérés 58
7.2.4 Étape 3: Identification des facteurs d'atténuation et des phénomènes physiques 59
7.2.5 Étape 4: Définition des séquences et conséquences et leur quantification 59
7.2.6 Étape 5: Analyse des conséquences 60
7.2.7 Étape 6: Utilisation des résultats de l'AAE 61
8 Évaluation 61
8.1 Remarques préliminaires 61
8.2 Analyse qualitative – Gestion des dépendances 62
8.2.1 Généralités 62
8.2.2 Dépendances fonctionnelles 62
8.2.3 Dépendances structurelles ou physiques 63
8.3 Analyse quantitative 65
8.3.1 Séquence indépendante d'événements 65
8.3.2 Liaison d'arbre de panne et réduction booléenne 66
9 Documentation 68
Annexe A (informative) Représentation graphique 69
Annexe B (informative) Exemples 71
Bibliographie 85

Figure 1 – Processus de développement des arbres d'événement 53
Figure 2 – Représentation graphique de base d'un arbre d'événement 62

Figure 3 – Dépendances fonctionnelles dans les arbres d'événement 63
Figure 4 – Modélisation des dépendances structurelles ou physiques 64
Figure 5 – Séquence d'événements 65
Figure 6 – Liaison d'arbre de panne 67
Figure A.1 – Représentation graphique souvent utilisée des arbres d'événement 69
Figure B.1 – Arbre d'événement d'un incendie classique dans un bâtiment de générateur diesel 73
Figure B.2 – Arbre d'événement simplifié en cas d'incendie 74
Figure B.3 – Système de passage à niveau (LX) 75
Figure B.4 – AAE d'un système de passage à niveau 77
Figure B.5 – Exemple simple 80
Figure B.6 – Arbre de panne pour la défaillance du système 1 80
Figure B.7 – Arbre de panne pour la défaillance du système 2 81
Figure B.8 – Arbre d'événement modifié 82
Figure B.9 – Arbre d'événement avec « pannes groupées » 83

Tableau A.1 – Éléments graphiques 70
Tableau B.1 – Symboles utilisés dans l'Annexe B 74
Tableau B.2 – Présentation du système 76
Tableau B.3 – Paramètres de réduction des risques pour les accidents de la Figure B.4 78

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

TECHNIQUES D'ANALYSE DE LA SÛRETÉ DE FONCTIONNEMENT – ANALYSE PAR ARBRE D'ÉVÉNEMENT (AAE)

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 elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
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 62502 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1380/FDIS	56/1389/RVD

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 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 stabilité 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.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La présente Norme internationale définit les principes et procédures de base de la technique de sûreté de fonctionnement désignée Analyse par Arbre d'Evénement (AAE).

La CEI 60300-3-1 répertorie de manière explicite l'AAE comme une méthode destinée à la sûreté de fonctionnement générale, ainsi qu'aux tâches d'analyse des risques et de la sécurité. L'AAE est également brièvement présentée dans la CEI 60300-3-9.

Les principes de base de cette méthodologie n'ont pas changé depuis la conception de la technique dans les années 60. L'AAE a été la première fois utilisée avec succès dans l'industrie du nucléaire dans une étude de l'U.S. Nuclear Regulatory Commission, le rapport WASH 1400 publié en 1975 [31][1].

Au cours des années suivantes, l'AAE a été largement acceptée comme méthodologie éprouvée d'analyse de la sûreté de fonctionnement et des risques. Elle a été appliquée dans divers secteurs de l'industrie (aéronautique, nucléaire, automobile, chimie, l'exploitation littoral pétrolière et gazière, l'industrie de la défense, les systèmes de transport).

A l'inverse de certaines techniques de sûreté de fonctionnement (le modèle Markov, par exemple), l'AAE repose sur des principes mathématiques relativement élémentaires. Toutefois, comme indiqué dans la CEI 60300-3-1, la mise en œuvre de l'AAE requiert un niveau élevé d'expertise quant à l'application de la technique. Cela est dû au fait qu'il faut être particulièrement attentif au traitement des événements dépendants. De plus, il est possible d'utiliser la relation étroite entre l'Analyse par Arbre de Panne (AAP) et l'analyse qualitative et quantitative des arbres d'événement.

La présente norme a pour objet de définir les principes de base consolidés de l'AAE et l'usage courant de cette technique comme moyen d'évaluation des mesures liées à la sûreté de fonctionnement et aux risques d'un système.

---

1 Les chiffres entre crochets se réfèrent à la bibliographie.

TECHNIQUES D'ANALYSE DE LA SÛRETÉ DE FONCTIONNEMENT – ANALYSE PAR ARBRE D'ÉVÉNEMENT (AAE)

1 Domaine d'application

La présente Norme internationale spécifie les principes de base consolidés de l'Analyse par Arbre d'Evénement (AAE) et donne les lignes directrices pour la modélisation des conséquences d'un événement initiateur, ainsi que pour l'analyse de ces conséquences d'un point de vue qualitatif et quantitatif dans le cadre de mesures liées à la sûreté de fonctionnement et aux risques.

Plus particulièrement, la présente norme traite des points suivants liés aux arbres d'événement:

a) définition des termes essentiels et description de l'utilisation des symboles et moyens de représentation graphique;

b) spécification des modes opératoires de construction de l'arbre d'événement;

c) élaboration des hypothèses, limites et avantages de l'analyse;

d) identification des relations avec d'autres techniques liées à la sûreté de fonctionnement et aux risques et explication des domaines d'applications pertinents;

e) proposition de lignes directrices pour les aspects qualitatifs et quantitatifs de l'évaluation;

f) des exemples pratiques.

La présente norme s'applique à tous les secteurs de l'industrie dans lesquels il est indispensable d'évaluer les mesures liées à la sûreté de fonctionnement et aux risques pour déterminer les conséquences d'un événement initiateur.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050-191:1990, *Vocabulaire Électrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 61025:2006, *Analyse par arbre de panne (AAP)*

3 Termes, définitions, abréviations et symboles

Pour les besoins du présent document, les termes et définitions suivants, ainsi que ceux donnés dans la CEI 60050-191, s'appliquent.

3.1 Termes et définitions

3.1.1
nœud
point de la représentation graphique de l'analyse par arbre d'événement décrivant au moins deux conséquences possibles pour le facteur d'atténuation

NOTE L'événement de tête de l'arbre de panne correspondant peut être directement lié à un nœud.

3.1.2
cause commune
cause d'apparition d'événements multiples
[CEI 61025:2006, 3.15]

NOTE Dans des situations particulières, il convient de spécifier le délai au cours duquel plusieurs événements se produisent, tels que "occurrence de plusieurs événements se produisant simultanément ou dans un intervalle de temps très rapproché".

EXEMPLES Les dangers naturels particuliers (par exemple, incendie, inondation), les défaillances d'un système de production, les infections biologiques ou les actes de l'homme.

3.1.3
événement
apparition d'une condition ou d'une action

[CEI 61025:2006, Définition 3.8]

3.1.4
en-têtes
facteurs d'atténuation énumérés au-dessus de la description de l'arbre d'événement

3.1.5
événement initiateur
événement à l'origine de l'arbre d'événement et de la séquence d'événements pouvant donner lieu à différentes conséquences possibles

3.1.6
facteur d'atténuation
système, fonction ou autre facteur circonstanciel atténuant les conséquences de l'événement initiateur

NOTE La plupart des secteurs industriels utilisent des termes spécifiques équivalents, par exemple, lignes de défense, lignes de protection, systèmes de protection, barrières de sécurité, lignes d'assurance, facteur de réduction des risques, etc.

3.1.7
conséquence
résultat possible de la séquence d'événements à la suite de la prise en compte de toutes les réactions des facteurs d'atténuation appropriés et compte tenu du fait qu'aucun autre développement de l'arbre d'événement n'est requis

3.1.8
séquence
chaîne d'événements, dont l'origine est l'événement initiateur, donnant lieu à une conséquence spécifique à la suite des événements résultants

3.1.9
événement de tête
événement indésirable prédéfini constituant le point de départ de l'analyse par arbre de panne et présentant l'intérêt principal pour l'analyse. Il se situe au sommet de la hiérarchie des événements sous lequel un arbre de panne est développé

NOTE C'est la conséquence de combinaisons de tous les événements d'entrée.

3.1.10
branche
représentation graphique de l'une des conséquences possibles provenant d'un nœud

3.2 Abréviations et symboles

3.2.1 Abréviations

ACC Analyse Causes-Conséquences

AAE Analyse par Arbre d'Evénement

AMDE Analyse des Modes de Défaillance et de leurs Effets

AAP Analyse par Arbre de Panne

IRF Risque Individuel d'Accident Mortel (IRF : *Individual Risk of Fatality)*

AELPAP Combinaison de deux techniques de sûreté de fonctionnement: Arbres d'Evénement Larges (AEL) et Petits Arbres de Panne (PAP)

LOPA Analyse des Niveaux de Protection[2]

BDF Blocs-Diagramme de Fiabilité (BDF)

ERP Evaluation du risque de probabilité

FP/AS Fiabilité Probabiliste/Analyse de la Sûreté

PAEAPL Combinaison de deux techniques de sûreté de fonctionnement: Petits Arbres d'Evénement (PAE) et Arbres de Panne Larges (APL)

3.2.2 Symboles

A Lorsqu'elles sont en italique, les lettres majuscules indiquent que l'événement A s'est produit.

$\overline{A}$ Lorsqu'elles sont en italique surmontées d'une barre, les lettres majuscules indiquent que l'événement A ne s'est pas produit.

I_E Lorsqu'il est en italique, ce symbole indique que l'événement initiateur s'est produit.

$O_{I_E,A,B}$ Ce symbole indique la conséquence, si tous les événements de l'indice (les lettres majuscules en italique étant reliées par des virgules) se sont produits dans l'ordre des événements indiqué dans l'indice (voir un exemple dans la Figure 3).

$\alpha,\ldots,\delta$ Les lettres grecques en minuscule indiquent des conséquences particulières de l'arbre d'événement.

« + » Ce symbole indique un opérateur logique « OU ».

« . » Ce symbole indique un opérateur logique "ET".

$P(A)$ Probabilité d'un événement A. P(A) est un nombre réel dans l'intervalle fermé [0,1] attribué à un événement (voir [25]).

$P(I_E.A.\overline{B}.\overline{C})$ Probabilité que l'événement initiateur I_E se soit produit et l'événement A se soit produit et l'événement B ne se soit pas produit et l'événement C ne se soit pas produit.

$P(A|I_E)$ Probabilité conditionnelle d'un événement A compte tenu de la survenue de l'événement initiateur I_E.

f Fréquence (nombre d'événements par unité de temps, voir [25]).

f_δ Fréquence de la conséquence δ .

---

2 LOPA: *Lafyers of Protection Analysis.*

4 Description générale

L'analyse par arbre d'événement (AAE) est un mode opératoire inductif permettant de modéliser les résultats possibles susceptibles de résulter d'un événement initiateur donné et de l'état des facteurs d'atténuation. Il s'agit également d'identifier et d'évaluer la fréquence ou la probabilité des différents résultats possibles d'un événement initiateur donné.

La représentation graphique d'un arbre d'événement requiert l'utilisation cohérente d'un ensemble de symboles, de repères et de libellés. Étant donné que la représentation des arbres d'événement varie en fonction des préférences de l'utilisateur, un ensemble de représentations graphiques communément utilisé est donné dans l'Annexe A.

En partant d'un événement initiateur, l'AAE pose la question « Que se passe-t-il si... « et construit un arbre des différentes résultats possibles. Il est donc fondamental de compiler une liste exhaustive des événements initiateurs afin de s'assurer que les arbres d'événement décrivent correctement toutes les séquences d'événements importantes du système considéré. Grâce à cette logique, l'AAE peut être décrite comme une méthode de représentation des facteurs d'atténuation en réponse à l'événement initiateur (en tenant compte des facteurs d'atténuation applicables).

D'un point de vue qualitatif, l'AAE permet d'identifier tous les scenarii accidentels potentiels (développement d'un arbre doté de branches de succès et de pannes) et les faiblesses potentielles de conception et de procédure. La branche de succès modélise la condition selon laquelle le facteur d'atténuation fonctionne comme prévu. A l'instar des autres techniques d'analyse, il est indispensable d'accorder une attention particulière à la modélisation des dépendances, en gardant à l'esprit que les probabilités utilisées pour quantifier l'arbre d'événement dépendent de la séquence d'événements antérieure à l'occurrence de l'événement concerné. L'Article 8 aborde ces aspects qualitatifs de l'analyse, ainsi que les règles quantitatives de base des calculs utilisés pour estimer les probabilités (sans dimension) ou les fréquences (1/h) de chacune des conséquences possibles. Bien qu'il soit, en théorie, possible de modéliser les effets des défaillances de l'opérateur ou du logiciel à l'aide d'un arbre d'événement, la présente norme ne porte pas sur leur quantification, ces questions étant abordées par d'autres publications de la CEI (CEI/PAS 62508 [23] et CEI 62429 [22], par exemple).

Les avantages de l'AAE, en tant que technique liée à la sûreté de fonctionnement et aux risques, et ses limites sont présentés dans l'Article 5. Comme exemple de limites de l'AAE, l'évolution chronologique doit être prise en compte avec circonspection. En effet, elle peut être traitée correctement uniquement dans des cas particuliers. Cette limite a donné lieu au développement de méthodes étroitement liées (la méthode d'analyse par arbre d'événement dynamique, par exemple) qui facilitent la modélisation des évolutions chronologiques. Cette méthode d'analyse par arbre d'événement dynamique n'est pas détaillée dans la présente norme, mais des références sont incluses dans la bibliographie pour plus d'informations.

L'AAE entretient une relation étroite avec l'analyse AAP, les événements de tête offrant une probabilité conditionnelle pour un nœud particulier de l'AAE. Cela est expliqué plus en détails dans l'Article 6, qui aborde également les relations entre l'AAE et d'autres techniques d'analyse (l'analyse causes-conséquences (ACC) et l'analyse des niveaux de protection (LOPA), par exemple). L'analyse causes-conséquences (ACC) combine l'analyse de cause et l'analyse de conséquence, d'où l'utilisation des approches déductives et inductives. La méthode LOPA a été développée par l'industrie de production par processus comme une adaptation particulière de l'AAE.

Étant donné que les premières étapes et qu'une approche bien construite sont essentielles au succès, l'Article 7 décrit le développement de l'arbre d'événement en commençant avec une définition précise du système. En outre, l'Article 7 aborde les différents aspects du système (techniques, opérationnels, humains et fonctionnels) ainsi que la profondeur de l'analyse. La manière d'établir la liste des événements initiateurs pertinents est également une question importante.

La Figure 1 présente les principales étapes d'une analyse par arbre d'événement. Malgré l'apparente simplicité du processus, l'analyste ne doit pas oublier que la construction d'un arbre d'événement est, sur de nombreux points, un processus itératif.

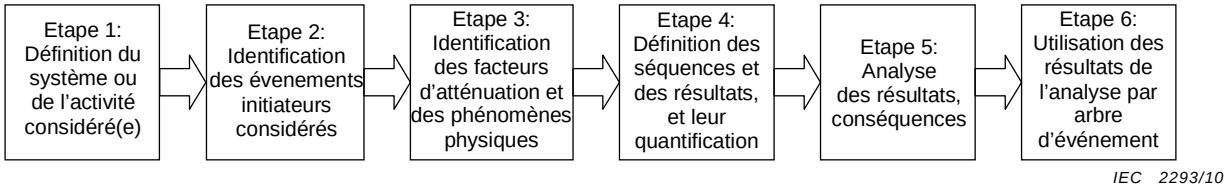

Figure 1 – Processus de développement des arbres d'événement

L'Article 9 présente brièvement la documentation requise pour l'analyse et les résultats.

L'Annexe A récapitule les représentations graphiques les plus communément utilisées pour les arbres d'événement. L'Annexe B donne des exemples d'AAE qui mettent en évidence son application dans de nombreux domaines, et donne des lignes directrices permettant de mener ces analyses.

5 Avantages et limites de l'AAE

5.1 Avantages

L'AAE offre les avantages suivants:

a) elle s'applique à tous les types de systèmes;

b) elle permet de visualiser les chaînes d'événements qui suivent un événement initiateur;

c) elle permet d'évaluer plusieurs pannes système simultanées (états se traduisant par l'impossibilité de réaliser une fonction requise, comme le défaut d'un système de surveillance) ou les défaillances (fin de la possibilité de réaliser une fonction requise, comme l'événement d'une soupape qui reste ouverte, par exemple) ainsi que d'autres événements dépendants;

d) elle fonctionne simultanément dans le domaine de défaillance ou de succès;

e) elle permet d'identifier les événements finaux imprévisibles par d'autres méthodes;

f) elle permet d'identifier les pannes localisées potentielles, les zones de vulnérabilité du système et les contre-mesures à faible efficacité. Cela permet d'optimiser le déploiement des ressources et d'améliorer le contrôle des risques par des modes opératoires et des fonctions de sécurité améliorés;

g) elle assure l'identification et la traçabilité des voies de propagation des pannes d'un système;

h) elle permet de décomposer des systèmes importants et complexes en petites parties plus faciles à gérer, regroupées en unités ou sous-systèmes fonctionnels plus petits.

L'avantage de l'AAE, par rapport à bien d'autres analyses et techniques liées aux risques, est son aptitude à modéliser la séquence et l'interaction des différents facteurs d'atténuation qui suivent l'occurrence de l'événement initiateur. Par conséquent, le système et ses interactions avec tous les facteurs d'atténuation d'un scénario d'accident se révèlent à l'analyste pour une meilleure évaluation des risques.

5.2 Limites

En général, les limites suivantes des techniques d'analyse de la sûreté de fonctionnement s'appliquent également à l'AAE:

a) les événements initiateurs ne sont pas révélés par l'analyse elle-même mais plutôt par la tâche analytique de la personne impliquée dans le processus de compilation d'une liste exhaustive d'événements initiateurs;

b) il revient à la personne impliquée dans le processus de compiler une liste exhaustive de scénarii de fonctionnement possibles;

c) les dépendances masquées du système risquent d'être ignorées, ce qui peut donner lieu à des estimations optimistes des mesures liées à la sûreté de fonctionnement et aux risques;

d) la méthode doit reposer sur l'expérience pratique de l'analyste et sur les investigations précédentes du système pour assurer le traitement correct des probabilités conditionnelles et des événements dépendants;

Les limites suivantes particulièrement applicables à l'AAE figurent ci-après:

e) l'aspect lié aux évolutions chronologiques dû à la dépendance temporelle des probabilités concernées peut être exactement traité si et seulement si les systèmes concernés ont une véritable probabilité constante de taux de panne ou si, dans le cas des stratégies de reprise et de réparation, l'indisponibilité en régime établi est rapidement atteinte. Il est important de tenir compte de cet élément avec les systèmes soumis régulièrement à essai;

f) un autre aspect délicat lié aux évolutions chronologiques est dû aux situations dynamiques (si les critères de réussite des facteurs d'atténuation varient en fonction de la manière dont les facteurs d'atténuation précédents ont échoué, par exemple). En règle générale, un cas classique est choisi pour refléter la situation;

g) un état particulier sur une période trop longue peut provoquer un état de panne, ce qui est difficile à modéliser dans un arbre d'événement (fuite lente d'un pneu, par exemple);

h) les dépendances de l'arbre d'événement dues, par exemple, aux dépendances entre l'événement initiateur et les facteurs d'atténuation, doivent faire l'objet d'une attention particulière. Toutefois, peu de techniques d'analyse sont à elles seules en mesure de traiter les dépendances (pannes dépendantes). La combinaison de l'analyse par arbre de panne et de l'analyse par arbre d'événement peut s'avérer avantageuse pour traiter ces aspects;

i) bien qu'il soit possible d'identifier plusieurs séquences de panne système, il peut être impossible de distinguer les niveaux de perte associés à des conséquences particulières sans procéder à une analyse supplémentaire. Toutefois, il est nécessaire d'avoir conscience de ces besoins.

6 Relation avec d'autres techniques d'analyse

6.1 Combinaison de l'AAE et de l'AAP

Dans la pratique, l'AAE est parfois réalisée comme une analyse autonome. Dans d'autres cas, elle l'est en combinaison avec l'AAP.

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 plus de détails, voir la CEI 61025.

Dans ce cas, par exemple, les défaillances de cause commune dans l'analyse quantitative peuvent être prises en compte, la combinaison de l'AAE et de l'AAP permettant de surmonter les faiblesses de l'AAE. Par conséquent, la combinaison de l'AAE et de l'AAP se traduit par une puissante technique d'analyse de la sûreté de fonctionnement et des risques.

La combinaison AAE/AAP est communément utilisée (parfois appelée ACC, pour Analyse Causes-Conséquences, voir [30] et [36]). Par exemple, l'AAP peut être utilisée pour évaluer la fréquence f d'un événement initiateur d'une AAE. Noter également que les probabilités conditionnelles des événements d'une séquence sont souvent calculées par l'AAP.

L'évaluation du risque de probabilité (ERP) est également un exemple de combinaison AAE/AAP destinée à une centrale nucléaire.

En principe, un événement initiateur peut être analysé par une AAE. Toutefois, dans certains cas, cela risque de ne pas être approprié pour les raisons suivantes:

a) les arbres résultants peuvent devenir très complexes;

b) il est parfois plus simple d'élaborer des relations causales plutôt que des conséquences d'événement;

c) ce sont souvent des équipes indépendantes qui dirigent l'analyse opérationnelle (les règles de procédure, par exemple) et l'analyse technique. Toutefois, l'interface et les dépendances entre le domaine opérationnel (les règles de procédure, les règles de maintenance par exemple) et le domaine technique ne sont pas toujours très claires au début de l'analyse. Ainsi pour les modes opératoires pratiques, les événements potentiels au niveau de l'interface entre le domaine opérationnel et technique sont définis en premier. En particulier, dans les applications de sécurité, il s'agit d'un mode opératoire standard, étant donné qu'en général, les pannes simples sont exclues par la conception (la sûreté intégrée, par exemple) et que, par conséquent, il convient qu'une analyse par arbre d'événement ne génère pas directement de conséquences graves par une panne individuelle sans autres facteurs d'atténuation possibles.

Il est possible de choisir entre deux approches de combinaison arbres d'événement/arbres de panne. Une approche est appelée AELPAP. Si l'arbre d'événement tend à devenir trop volumineux, l'approche PAEAPL peut être utilisée.

Dans l'approche AELPAP, les états de tous les systèmes qui prennent en charge le système en cours d'analyse, ici appelé système de soutien, apparaissent de manière explicite dans les arbres d'événement. Les événements de tête des arbres de panne comportent des conditions aux limites associées, incluant l'hypothèse selon laquelle le système de soutien se trouve dans un état particulier correspondant à la séquence d'événements en cours d'évaluation. Pour chaque système donné, des arbres de panne distincts sont utilisés pour chaque ensemble de conditions aux limites. Ils peuvent être générés à partir d'un seul arbre de panne incluant les systèmes de soutien et qui, avant d'être associé à une séquence particulière, est « conditionné » sur l'état du système de soutien associé à cette séquence. Cette approche génère une AELPAP qui représente explicitement les dépendances existantes. Puisqu'elles sont associées à des arbres de panne plus petits, elles nécessitent moins de ressources informatiques et de programmes informatiques sophistiqués. Toutefois, la complexité des arbres d'événement augmente rapidement en raison des combinatoires avec le nombre de systèmes de soutien et le nombre d'états de système de soutien explicitement décrits dans l'arbre. De plus, le processus de quantification est plus lourd et peut faire l'objet d'omissions. Il convient également de considérer que l'approche AELPAP n'identifie pas de manière explicite les combinaisons particulières de pannes du système de soutien (également appelé système linéaire) donnant lieu à une défaillance du système. Un exemple simplifié de ce type d'arbre d'événement large est présenté à la Figure B.1. Voir [31] pour plus de détails.

Dans l'approche PAEAPL, les arbres d'événement avec les fonctions d'événement initiateur et d'atténuation comme en-têtes sont en premier lieu développés, puis étendus aux arbres d'événement avec l'état des systèmes linéaires comme en-têtes. Les modèles d'arbre de panne du système linéaire sont développés vers les limites appropriées avec les systèmes de soutien. Les arbres de panne du système de soutien peuvent être développés séparément et intégrés à un stade ultérieur dans les modèles de système linéaire. Cette approche génère des arbres d'événement concis qui permettent de créer une vue synthétique d'une séquence d'accidents. De plus, en fonction de la disponibilité des programmes informatiques, les petits arbres d'événement peuvent être plus facilement numérisés. Toutefois, les dépendances et l'importance correspondante des systèmes de soutien ne sont pas explicitement apparentes. Un exemple théorique de ce type de petit arbre d'événement est présenté à la Figure B.5. Voir [4] pour plus de détails.

6.2 Analyse des niveaux de protection (LOPA)

L'analyse LOPA est une forme particulièrement normalisée de l'AAE. Elle est utilisée comme un moyen simplifié d'analyse des risques d'un environnement d'application particulier. L'analyse LOPA se présente sous la forme d'une fiche technique analogue à l'AMDE: les événements initiateurs sont enregistrés dans des lignes, et les différentes couches de protection (représentant les facteurs d'atténuation normalisés) dans des colonnes. Cela signifie qu'une séquence d'événements d'une analyse LOPA peut également être traitée comme une AAE. Pour les besoins de l'analyse des risques, les mesures de la gravité (ou des dommages) sont également intégrées dans la fiche technique.

Par conséquent, l'analyse LOPA peut être considérée comme une AAE avec un ensemble limité de facteurs d'atténuation possibles adaptés à un environnement d'application particulier. Elle est le plus souvent utilisée dans la production par processus. Plus de détails sur l'analyse LOPA sont disponibles en [1] et [5].

6.3 Combinaison avec d'autres techniques

L'AAE peut être combinée avec toute autre technique utile pour déduire la probabilité de succès ou d'échec des facteurs d'atténuation correspondants (les techniques de Markov ou les blocs-diagramme de fiabilité (BDF), par exemple, voir [16]), mais dans ces cas, les autres techniques viennent uniquement en complément de l'AEE.

Dans le cas des dépendances non essentielles et temporelles du comportement du système (voir 8.3.2), il est possible de recourir aux techniques de Markov si ses autres limites spécifiques sont prises en compte. Pour plus de détails, voir [17].

L'Analyse des modes de défaillance et de leurs effets (AMDE) est une autre technique étroitement liée d'analyse de la sûreté de fonctionnement, voir [13]. Il s'agit d'un mode opératoire formel et systématique d'analyse du système visant à identifier les modes de défaillance potentiels, leurs causes et leurs effets sur les performances du système. En règle générale, l'AMDE permet d'identifier la gravité des modes de défaillance potentiels, et de faire en sorte que la conception intègre les facteurs d'atténuation afin de réduire les probabilités de défaillance du système ou de la fonction à un niveau acceptable. Il peut s'agir de la première étape du développement d'un arbre d'événement, identifiant les défaillances cruciales d'un système comme événements initiateurs possibles.

La modélisation de Markov, le BDF et l'AMDE sont normalisés dans la CEI 61165 [17], la CEI 61078 [16] et la CEI 60812 [15].

7 Développement des arbres d'événement

7.1 Généralités

Les événements qui déterminent les séquences d'événements se caractérisent en général en termes de:

a) fonctions: la réalisation (ou non) des fonctions en tant que facteurs d'atténuation;

b) systèmes: l'intervention (ou non) des systèmes en tant que facteurs d'atténuation supposés exécuter une action visant à empêcher la progression de l'événement initiateur vers un accident ou en cas de défaillance des facteurs d'atténuation, à atténuer l'accident lui-même;

c) phénomène: l'occurrence ou la non-occurrence de phénomènes physiques.

En règle générale, les fonctions nécessaires suivant un événement initiateur sont identifiées en premier, puis les systèmes (facteurs d'atténuation) qui peuvent réaliser ces fonctions. Les phénomènes physiques décrivent l'évolution à l'intérieur et à l'extérieur du système considéré (les transitoires de pression et de température, les incendies, les dispersions toxiques, par exemple).

Il convient de définir clairement le domaine d'application et l'objet de l'AAE avant d'aborder les étapes détaillées de 7.2.

7.2 Étapes de l'analyse par arbre d'événement

7.2.1 Mode opératoire

Le mode opératoire de réalisation d'une AAE (voir Figure 1) est composé des six étapes ci-dessous:

Étape 1: Définition du système ou de l'activité considéré(e) (voir 7.2.2)

Préciser et définir clairement les limites du système ou de l'activité pour lequel les AAE sont réalisées.

Étape 2: Identification des événements initiateurs considérés (voir 7.2.3)

Procéder à un dépistage afin d'identifier les événements importants ou les catégories d'événements que l'analyse va aborder. Les catégories comprennent, par exemple, les collisions, les incendies, les explosions, les émanations toxiques, etc.

Étape 3: Identification des facteurs d'atténuation et des phénomènes physiques (voir 7.2.4)

Identifier les différents facteurs d'atténuation qui peuvent influencer la progression de l'événement initiateur vers son résultat. Ces facteurs d'atténuation comprennent les systèmes de production et les actions/décisions de l'homme. De même, identifier les phénomènes physiques ou les événements circonstanciels (l'inflammation ou les conditions climatiques qui affectent la progression et la conséquence de l'événement initiateur, par exemple). L'arbre d'événement repose sur l'intégration de tous ces facteurs d'atténuation et phénomènes physiques (voir 7.1).

Étape 4: Définition des séquences et conséquences et leur quantification (voir 7.2.5)

Pour chaque événement initiateur, définir les différentes conséquences (scénarii d'accident, par exemple) qui peuvent se produire, et procéder à l'analyse quantitative réelle sur la base de l'arbre d'événement construit.

Étape 5: Analyse des conséquences (voir 7.2.6)

Les différentes conséquences sont analysées en fonction de leurs conséquences et de leur impact sur les résultats de l'analyse.

Étape 6: Utilisation des résultats de l'analyse par arbre d'événement (voir 7.2.7)

Les constatations qualitatives et quantitatives de l'analyse sont traduites en actions nécessaires.

7.2.2 Étape 1: Définition du système ou de l'activité considéré(e)

Une AAE porte sur les différents cheminements faisant qu'un événement initiateur engendre des accidents à la suite de défaillances des différents facteurs d'atténuation. Par conséquent, l'identification et la recherche attentives des facteurs d'atténuation constituent une première étape importante de l'évaluation de l'efficacité d'un facteur d'atténuation.

Très peu de systèmes fonctionnent, en pratique, de manière isolée. La plupart des systèmes sont reliés à d'autres systèmes ou interagissent avec eux. En définissant clairement les limites, en particulier avec des systèmes de soutien tels que les systèmes d'alimentation en énergie électrique et l'air comprimé, les analystes peuvent éviter d'oublier des éléments essentiels d'un système au niveau des interfaces, ou de pénaliser un système en associant par inadvertance d'autres équipements à l'objet de l'étude.

Du point de vue conceptuel, les AAE peuvent inclure tous les événements et toutes les conditions pouvant contribuer à une conséquence particulière ou peuvent assurer un certain niveau de protection contre les accidents considérés. Toutefois, il n'est pas pratique d'inclure toutes les contributions possibles dans l'étude. La plupart des analyses définissent des limites analytiques qui

a) limitent le niveau de résolution analytique (l'analyste peut, par exemple, décider de ne pas analyser en détail tous les problèmes du système de distribution électrique lors de l'étude d'un système de navigation);

b) excluent de manière explicite certains types d'événements ou de conditions (le sabotage, par exemple) de l'analyse.

L'état initial d'un système, notamment les équipements supposés hors service au départ, gêne les combinaisons d'événements nécessaires à la génération de conséquences subséquentes. Par exemple, si un verrouillage de protection est régulièrement retiré, l'arbre d'événement doit être ajusté de manière à refléter les scénarii modifiés, en raison d'un risque potentiellement accru.

7.2.3 Étape 2: Identification des événements initiateurs considérés

En règle générale, cette étape implique l'utilisation d'une vaste technique d'identification des dangers (une analyse par hypothèse, une évaluation préliminaire ou une analyse préliminaire des risques, par exemple). Il s'agit d'évaluer systématiquement toutes les activités entrant dans le domaine d'application de l'étude (la prise en compte de l'expérience opérationnelle dans le domaine du secteur spécifique, par exemple). Cette étape permet d'identifier les dangers et les événements initiateurs possibles qui en découlent. Ces méthodes d'identification considèrent, dans une large mesure, toutes les opérations entrant dans le domaine d'application de l'étude et cherchent à identifier l'éventail complet des événements initiateurs et des conséquences qui leur sont associées. Pour obtenir une liste exhaustive et la description des différentes méthodes, voir [12]. La conséquence de ces processus d'identification est en général une liste exhaustive des événements potentiels et de leurs conséquences prévues.

Dès lors, il convient d'identifier la totalité du spectre des événements qui peuvent se produire et entrant dans le domaine d'application de l'analyse. Par la suite, les analystes appliquent des critères de dépistage afin d'identifier les événements initiateurs les plus intéressants qui seront analysés avec les arbres d'événement. Fondamentalement, il existe deux possibilités d'élimination d'événements initiateurs, à savoir l'exclusion en raison des propriétés physiques peu probables (les valeurs de charge de pression, de température et calorifiques ne sont pas dépassées, par exemple) ou en raison des faibles fréquences de l'événement initiateur en général estimées de manière prudente. Cette étape permet d'identifier les événements à analyser plus en profondeur afin de comprendre les interactions complexes des systèmes. Au cours de l'analyse, il convient de vérifier la possibilité d'interaction entre les événements initiateurs et les facteurs d'atténuation (si l'environnement tel qu'il a été généré par l'événement initiateur, comme la coupure d'alimentation électrique à la suite d'un séisme, peut affecter de manière préjudiciable les performances des facteurs d'atténuation, par exemple).

A la suite de l'identification et du dépistage de la liste initiale des événements, le reste de la liste des événements initiateurs contient les éléments qui seront analysés avec les arbres d'événement. Il s'agit d'événements que des experts compétents ont identifiés comme étant suffisamment complexes pour nécessiter une analyse supplémentaire des différentes interactions entre le système et le personnel à l'origine des conséquences provenant de l'événement initiateur.

Si de nombreux événements sont analysés avec les arbres d'événement, il convient de regrouper les événements initiateurs en différentes catégories (collisions, incendies, explosions, émanations toxiques, etc. par exemple). Dans certains cas, ce classement d'événements peut ne pas être applicable. Par exemple, si l'étude a pour objet d'identifier l'éventail des conséquences associées uniquement aux incendies, il convient que l'analyse de

dépistage réalisée à l'étape précédente ait permis d'éliminer tous les événements n'étant pas liés aux incendies, de sorte que la dernière étape du classement des événements ne soit pas nécessaire.

Les événements initiateurs regroupés dans la même classe impliquent l'intervention des mêmes facteurs d'atténuation et donnent lieu à des conséquences similaires.

7.2.4 Étape 3: Identification des facteurs d'atténuation et des phénomènes physiques

Une fois un événement initiateur défini, tous les facteurs d'atténuation requis pour atténuer les scénarii de conséquences ou d'accidents doivent être définis et organisés en fonction de leur durée d'intervention. Il s'agit de composants d'ingénierie (alarmes, verrouillages et soupapes automatiques, par exemple) et de systèmes d'administration ou de gestion du personnel (sapeurs-pompiers, urgences et détection humaine par la vue, le toucher, l'ouïe ou l'odorat par exemple).

Ces fonctions réalisées par les composants ou facteurs d'atténuation susmentionnés sont structurées sous la forme d'en-têtes dans l'arbre d'événement fonctionnel. Pour chaque fonction, l'ensemble de succès et échecs possibles doit être identifié et recensé. Chaque ensemble de succès ou d'échecs, respectivement, associé à un facteur d'atténuation engendre l'apparition d'une branche dans l'arbre d'événement, qui n'est pas nécessairement limitée à un nœud à deux branches.

Les phénomènes physiques, parfois appelés événements phénoménologiques, peuvent également influencer la conséquence d'un événement initiateur. Par exemple, en cas d'émanation d'un liquide inflammable, des dispositifs de sécurité peuvent être conçus pour isoler la fuite. Toutefois, si la fuite n'est pas isolée, la dernière conséquence de l'émanation est influencée par différentes réponses physiques (allumage immédiat, allumage différé ou caractéristiques de dispersion, par exemple). Ces réponses physiques sont également modélisées sous forme de nœuds dans les arbres d'événement.

Dans une analyse système nécessitant plusieurs arbres d'événement correspondant à plusieurs événements initiateurs, il est possible de simplifier la génération de ces arbres d'événement en les classant en fonction des facteurs d'atténuation. Cela permet de répéter la même logique d'arbre d'événement (c'est-à-dire les facteurs d'atténuation avec le même échec ou succès) pour différents événements initiateurs considérés. Si les facteurs d'atténuation répondent de la même manière à différents événements, il est généralement possible de faire la somme des fréquences d'événements individuels pour parvenir à une fréquence représentative de tous les événements de cette classe. Pour plus d'informations sur l'analyse quantitative, voir 8.3.

7.2.5 Étape 4: Définition des séquences et conséquences et leur quantification

Comme indiqué plus haut, l'un des avantages de la technique AAE est son aptitude à modéliser l'ordre d'intervention et d'interaction des différents systèmes répondant à l'événement initiateur. Par conséquent, l'intervention des différents systèmes peut être modélisée « l'un après l'autre ». Pour tenir compte suffisamment de ces interactions, l'analyste doit

– déterminer la progression logique de l'événement initiateur par l'intermédiaire des différents facteurs d'atténuation en fonction des scénarii des conséquences/accidents possibles,
– identifier les dépendances entre les facteurs d'atténuation,
– prendre en compte les réponses conditionnelles d'un système, compte tenu de l'action des systèmes précédents,
– construire l'arbre d'événement pour résoudre les éléments ci-dessus.

Il est certain que tous les événements initiateurs (pannes du système, par exemple) n'engendrent pas des conséquences catastrophiques. De même, tous les facteurs

d'atténuation ou verrouillages ne sont pas appelés à répondre à tous les événements qui se produisent. Il existe une progression logique à une séquence d'accidents à partir du moment où l'événement initiateur se produit. Au fur et à mesure de la progression de la séquence d'accidents et de l'augmentation de sa gravité, les systèmes répondent de différentes manières. Il est essentiel de bien mesurer la progression et la séquence du système et de la réponse physique afin de développer la logique correcte dans l'arbre d'événement. Par exemple, si un feu se déclenche par combustion spontanée dans une corbeille à papier, la réponse initiale consiste à éteindre le feu avec des extincteurs, si des personnes sont présentes et si des extincteurs sont disponibles. L'ensemble du système de protection incendie et la réponse des pompiers n'interviennent pas tant que la gravité de l'accident n'a pas augmenté.

La plupart des systèmes sont connectés à d'autres systèmes et processus ou interagissent avec eux. Ces interactions, ou dépendances, influencent (dégradent) le niveau de protection des systèmes redondants partageant certains équipements. Par exemple, sur un pétrolier doté de systèmes de direction et de propulsion redondants, les pannes de chaque système peuvent ne pas être indépendantes si les systèmes de direction partageaient une conduite d'alimentation hydraulique commune.

Les arbres d'événement impliquent des probabilités conditionnelles. En d'autres termes, la probabilité d'une réponse spécifique (succès ou échec, par exemple) d'un facteur d'atténuation repose sur la réponse spécifique du facteur d'atténuation qui le précède.

Le processus de construction recommandé pour l'arbre d'événement est composé des étapes suivantes:

a) placer l'événement initiateur sur le côté gauche de l'arbre;

b) placer les facteurs d'atténuation et les phénomènes physiques en haut de l'arbre, dans l'ordre chronologique dans lequel ils affectent la progression d'accidents, par exemple;

c) identifier les succès (qui s'affichent en général dans la branche du haut) et les échecs (branche du bas) de chaque facteur d'atténuation au niveau de chaque nœud en tenant compte de ce qui suit:

   1) certains nœuds peuvent comporter plus de deux conséquences et présentent le nombre approprié de branches (voir Annexe A);

   2) certains nœuds ne comportent qu'une seule conséquence. En d'autres termes, ces facteurs d'atténuation sont reliés par une ligne droite. Cela est le cas lorsque la probabilité conditionnelle est de 1,0. Le facteur d'atténuation n'affecte pas la conséquence, en raison de certains succès ou échecs précédents d'un autre facteur d'atténuation.

Ces étapes sont illustrées de manière plus détaillée dans l'Annexe A, et en termes généraux et de manière plus spécifique dans les Figures B.1 et B.4, avec des exemples dans le domaine des réseaux ferroviaires et des centrales électriques.

L'analyse quantitative est présentée plus en détail en 8.3 et dans un exemple en B.2.6.

7.2.6 Étape 5: Analyse des conséquences

Les conséquences d'AAE sont déterminées par l'extrémité de chaque branche de l'arbre d'événement. Chaque conséquence peut être évaluée de manière qualitative ou quantitative. Dans le premier cas, la conséquence identifie les différentes séquences d'événements dues à l'occurrence de l'événement initiateur étudié. L'évaluation quantitative offre un meilleur aperçu de l'importance relative des facteurs d'atténuation car, dans ce cas, la conséquence est représentée par une fréquence. Pour quantifier l'analyse par arbre d'événement, il est nécessaire de disposer de données d'occurrence d'événement adéquates, suffisantes et fiables.

Il s'avère parfois avantageux de diviser les conséquences possibles en différentes catégories, en fonction du type particulier de dommage (pertes en vies humaines, dommages matériels, atteinte à l'environnement ou importance des dégâts, dommage dû aux carburants). Le nombre de conséquences de l'arbre d'événement est déterminé en définissant les types de conséquences à analyser, par exemple:

a) états de panne ou de dommage du système;

b) destruction du système;

c) gravité de l'impact sur l'environnement; ou

d) perte en vies humaines.

Pour procéder à l'évaluation pratique des conséquences multiples, il est utile de classer et de grouper les conséquences comparables, de manière à simplifier les résultats.

7.2.7 Étape 6: Utilisation des résultats de l'AAE

Les résultats de l'analyse par arbre d'événement peuvent permettre de formuler une base de prise de décision et de choisir des solutions optimales en matière de sécurité, afin d'améliorer la sûreté de fonctionnement et de réduire les risques sur une base technique et organisationnelle solide. Les actions correctives peuvent impliquer de modifier l'architecture du système, les procédures d'exploitation et de maintenance, etc.

En particulier, il est possible de récapituler les décisions reposant sur l'analyse réalisée de la manière suivante:

a) aptitude à évaluer la tolérabilité ou l'acceptabilité du risque: les résultats tenant compte des dommages connexes en raison de critères d'acceptabilité du risque pertinents sont-ils tolérables?

b) améliorations potentielles: identifier les facteurs de réduction des risques et les modifications pertinentes apportées à l'architecture du système examiné afin de satisfaire aux critères d'acceptabilité;

c) recommandations pour l'amélioration: développer des suggestions particulières d'amélioration des performances, y compris

   1) modification des équipements,

   2) modifications de mode opératoire,

   3) modification des règles administratives (tâches de maintenance planifiées, formation du personnel, etc. par exemple).

d) justification d'allocation des ressources: estimer dans quelle mesure la mise en œuvre des recommandations pour l'amélioration affecte les performances.

Étant donné que le système analysé peut faire l'objet de modifications tout au long de sa durée de vie, il convient de maintenir à jour l'AAE tout au long du cycle de vie du système afin de faciliter le processus de prise de décision. Dans certains secteurs de l'industrie, ce processus de mise à jour périodique régulier est appelé « FP/AS vitale » (Fiabilité Probabiliste/Analyse de la Sûreté). L'imbrication nécessaire des analyses dans le processus général de gestion des risques est présentée plus en détail dans [12].

8 Évaluation

8.1 Remarques préliminaires

Avant de commencer l'analyse quantitative de la fréquence ou de la probabilité des conséquences des différentes séquences d'événements, il est indispensable d'analyser avec soin les aspects qualitatifs du modèle d'arbre d'événement. Ils comprennent la dépendance des événements, y compris l'événement initiateur et les événements de tête, ainsi que les événements intermédiaires ou de base des arbres de panne liés.

Afin de faciliter la description des principes de base de l'évaluation, la Figure 2 illustre la représentation graphique de base d'un arbre d'événement pour les besoins de l'illustration.

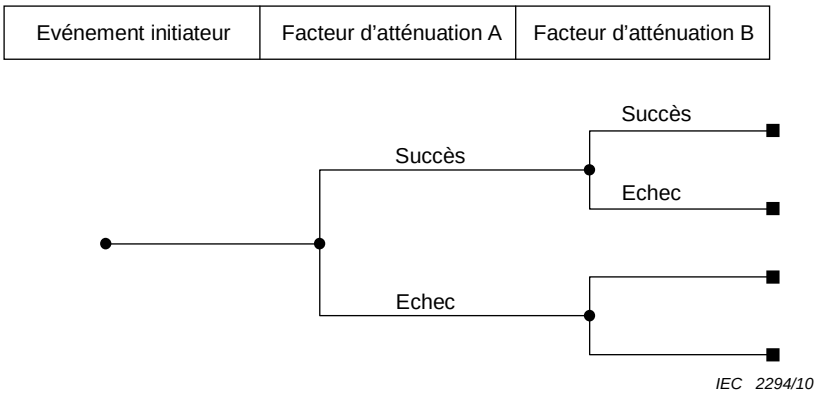

Figure 2 – Représentation graphique de base d'un arbre d'événement

8.2 Analyse qualitative – Gestion des dépendances

8.2.1 Généralités

Les objectifs de l'analyse qualitative peuvent être résumés comme suit:

a) comprendre les facteurs susceptibles de déterminer une dépendance entre des fonctions ou entre les composants d'un système;

b) identifier les événements de panne secondaire potentielle importants;

c) faciliter l'analyse quantitative correcte de l'arbre d'événement et établir le lien avec les arbres de panne.

L'analyse qualitative, et en particulier l'analyse des dépendances, est abordée dans d'autres articles afin d'insister sur son importance, et non parce qu'elle doit être réalisée séparément de l'analyse de séquence d'événements et de l'analyse des systèmes.

Les dépendances présentent deux aspects principaux, à savoir:

– les dépendances fonctionnelles (voir 8.2.2);

– les dépendances structurelles ou physiques (voir 8.2.3).

Par exemple, les dépendances peuvent être fonctionnelles si la défaillance d'un facteur d'atténuation à intervenir empêche également l'intervention de celui qui lui succède (si les facteurs d'atténuation partagent certains composants dont le dysfonctionnement les met hors d'état de fonctionner, par exemple). De plus amples informations sur cette distinction sont disponibles en [40].

Pour simplifier, les arbres d'événement qui suivent se trouvent au niveau du système.

8.2.2 Dépendances fonctionnelles

L'ordre des différents facteurs d'atténuation dans la séquence de l'arbre d'événement n'est pas uniquement déterminé par le moment de leur intervention en tant que facteur d'atténuation possible, mais également par leur ordre logique. Il est essentiel de savoir que l'intervention réussie d'un facteur d'atténuation dépend du succès de l'intervention d'un autre. Cela pourrait être le cas, par exemple, si

a) un facteur d'atténuation représente un système de soutien pour l'autre, ou

b) en cas de modification des paramètres environnementaux susceptibles d'affecter le succès ou l'échec de l'autre facteur d'atténuation.

Par exemple, soit l'arbre d'événement de la Figure 3, dans lequel les pannes subséquentes des systèmes A et B (facteurs d'atténuation) donnent les conséquences illustrées. Dans cet exemple, le système A est pris en charge par le système B.

Après la réorganisation des systèmes A et B dans l'arbre d'événement (voir la Figure 3), il n'est pas utile de décomposer la branche qui suit la défaillance du système B en deux branches pour le système A, la défaillance du système B impliquant l'impossibilité du système A à remplir sa fonction. Cela permet d'élaguer l'arbre d'événement. Étant donné que cette opération est la plupart du temps réalisée par des programmes informatiques, l'analyste a pour principale mission de considérer les différentes dépendances du modèle.

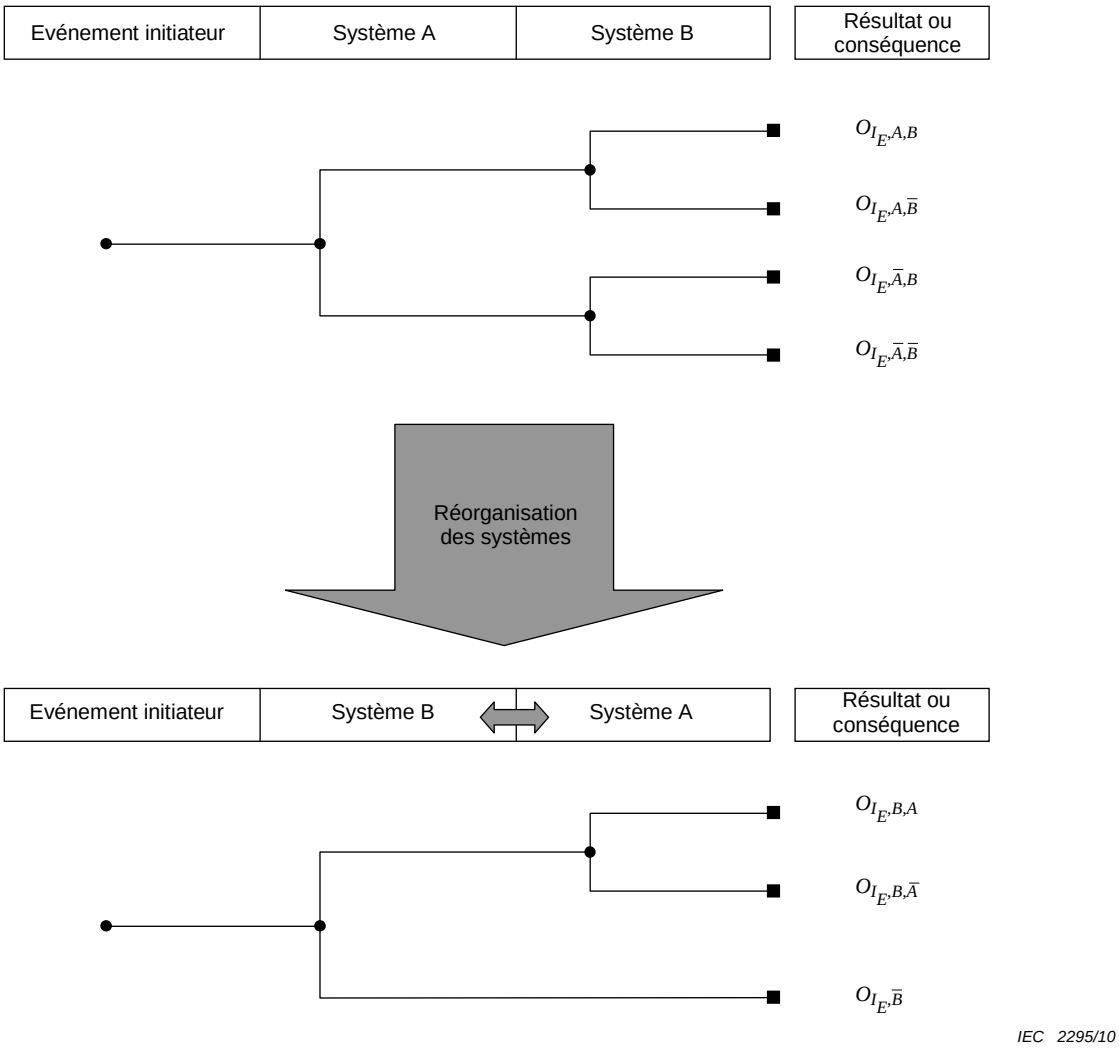

Figure 3 – Dépendances fonctionnelles dans les arbres d'événement

Avant d'appliquer le processus de réorganisation, il est essentiel de ne pas oublier que la représentation de l'arbre d'événement peut modéliser une séquence temporelle particulière de la défaillance des systèmes. Par conséquent, l'arbre d'événement particulier ne modélise pas le domaine complet des séquences temporelles possibles après l'événement initiateur. Il est indispensable de tenir compte de cet élément une fois les outils de liaison d'arbre de panne ou les méthodes booléennes (8.3.2 et Clause B.2) sont appliqués.

8.2.3 Dépendances structurelles ou physiques

En règle générale, les dépendances structurelles ou physiques donnent lieu à des défaillances de cause commune. De même, ces défaillances de cause commune génèrent

plusieurs événements (voir la définition 3.1.2). Les défaillances de cause commune sont par exemple des défaillances provoquées par des événements tels que des incendies, des séismes, des ouragans, des défaillances de systèmes de production (une défaillance ou l'explosion massive d'une centrale électrique, d'origine interne ou externe par exemple) ou des actes humains (erreurs humaines ou actes de violence par exemple).

Par conséquent, une analyse de cause commune est réalisée pour déterminer la susceptibilité de défaillance des différents facteurs d'atténuation à partir de conditions, de systèmes ou de fonctions externes ou internes.

La question est de savoir si l'occurrence d'un événement initiateur (un séisme, par exemple) affecte les probabilités conditionnelles d'occurrence de tous les événements de tête des arbres de panne liés (voir 8.3.2).

Une autre étape de l'analyse qualitative consiste à identifier les systèmes communs ou les fonctions communes qui influencent les différents facteurs d'atténuation. Considérons, par exemple, un arbre d'événement dans lequel la défaillance du système A suivie d'une défaillance du système B donne lieu à une conséquence non souhaitée. Si le système A s'appuie sur une partie du système B pour fonctionner correctement, il est possible d'extraire la « partie commune » et de considérer trois systèmes: les systèmes A* et B*, qui sont les systèmes A et B sans les parties communes, et le système C, qui représente les parties communes utilisées par les systèmes A et B. Ce scénario est illustré à la Figure 4.

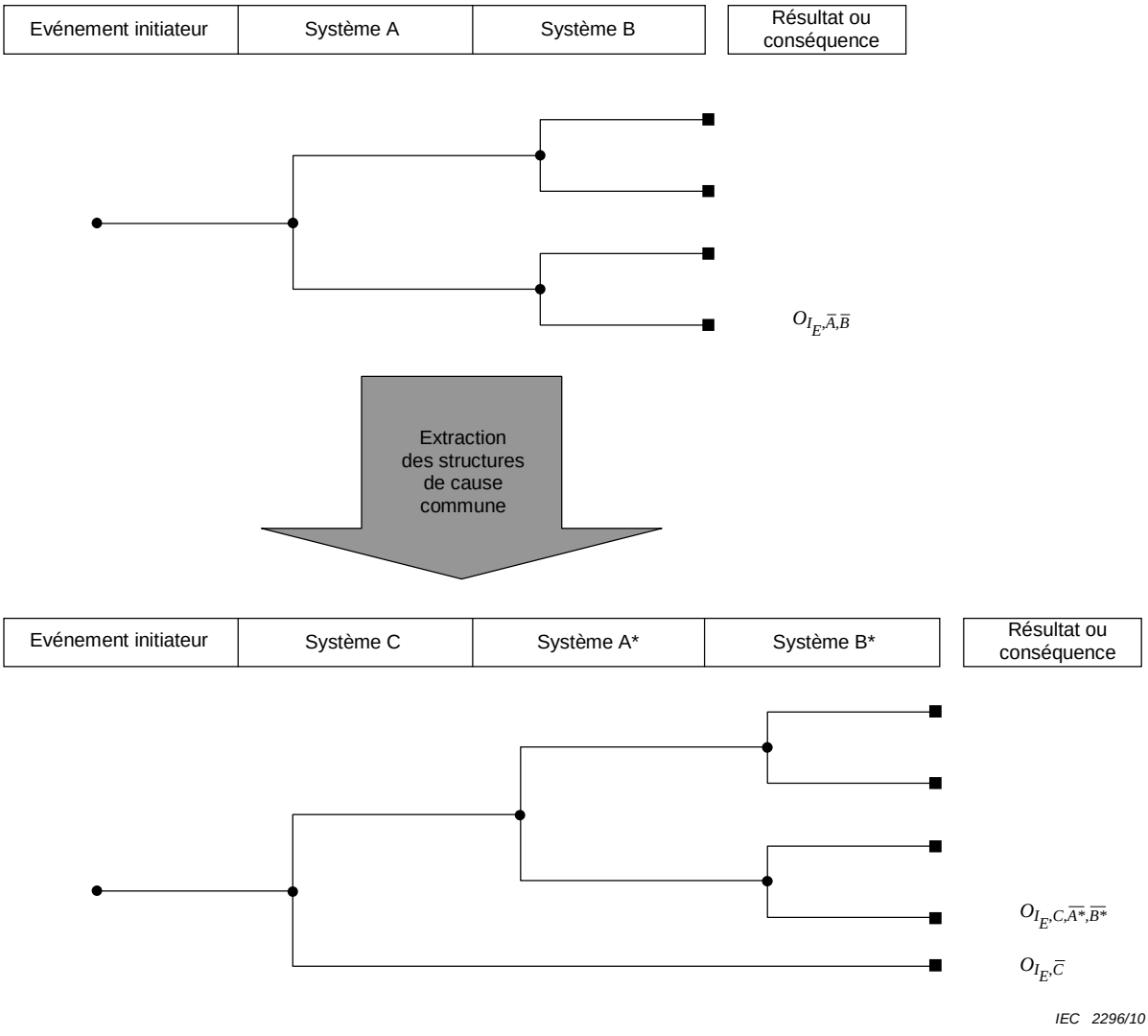

Figure 4 – Modélisation des dépendances structurelles ou physiques

Dans la plupart des cas, les dépendances sont beaucoup plus complexes que celles présentées ci-dessus.

Par exemple, les défaillances provoquées par des actions de maintenance réalisées par des membres de la même équipe ne peuvent pas être modélisées aisément comme indiqué ci-dessus. Dans le cas de combinaisons multiples de systèmes dépendants et de leurs composants, il est possible de recourir à la liaison d'arbre de panne, décrite en détails en 8.3.2.

8.3 Analyse quantitative

8.3.1 Séquence indépendante d'événements

Lorsque toutes les probabilités conditionnelles de succès ou d'échec des facteurs d'atténuation sont indépendantes les unes des autres, l'analyse quantitative devient simple.

Soit un arbre d'événement comportant les trois facteurs d'atténuation – les systèmes A, B et C. La Figure 5 présente une séquence particulière de l'arbre d'événement résultant (illustrée par une ligne en pointillés), dans laquelle le système A fonctionne, alors que les systèmes B et C sont en panne. Les alinéas suivants expliquent les principes de base de l'évaluation de la fréquence ou de la probabilité de conséquence de cette séquence δ particulière. Des exemples pratiques des arbres d'événement sont donnés ci-après.

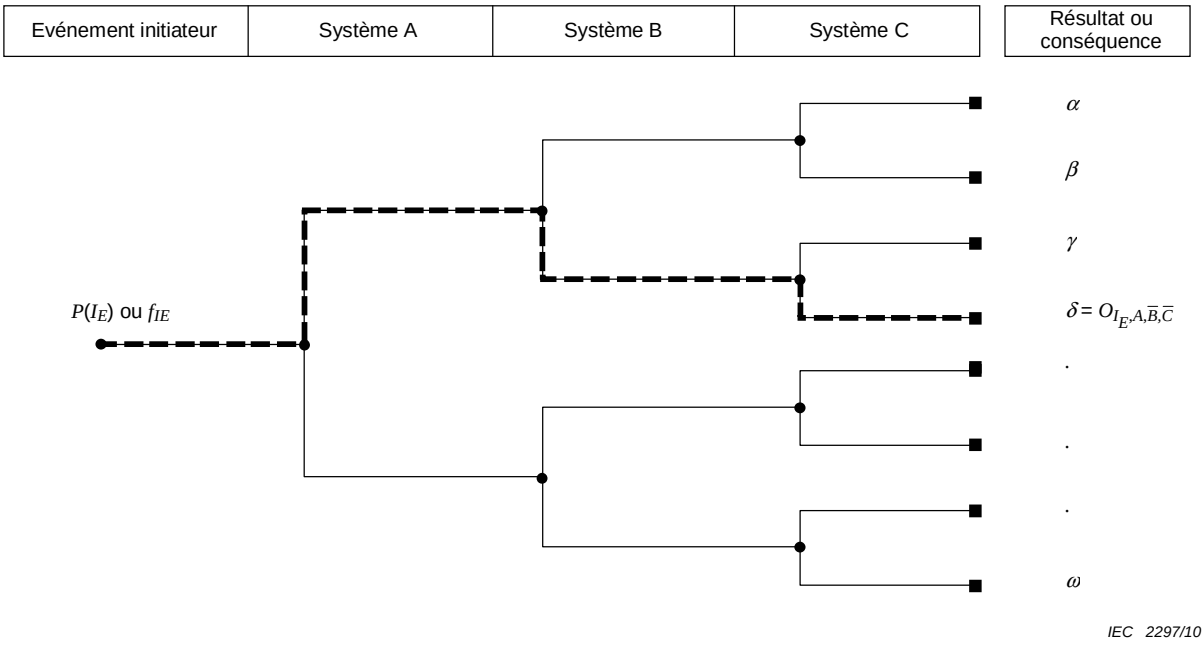

Figure 5 – Séquence d'événements

Le théorème de probabilité conditionnelle peut être utilisé avec les définitions de l'Article 3 pour écrire l'Equation (1) pour la probabilité $P(\delta)$ de cette séquence δ particulière:

$$\begin{aligned} P(\delta) &= P\left(I_E \times A.\overline{B}.\overline{C}\right) \\ &= P(I_E) \times P(A \mid I_E) \times P\left(\overline{B} \mid I_E.A\right) \times P\left(\overline{C} \mid I_E.A.\overline{B}\right) \end{aligned} \quad (1)$$

où

$P(I_E)$ est la probabilité d'occurrence de l'événement initiateur I_E,

$P(A \mid I_E)$ est la probabilité de succès du système A compte tenu de l'occurrence de l'événement initiateur I_E (probabilité conditionnelle).

Si les succès et échecs d'un système sont indépendants de ceux des autres systèmes, il est possible de recourir aux probabilités conditionnées uniquement par l'événement I_E. Par conséquent, l'Equation (1) peut être simplifiée comme suit avec $P(I_E)$ comme probabilité d'occurrence de l'événement initiateur:

$$P(\delta) = P(I_E) \times P(A \mid I_E) \times P(\overline{B} \mid I_E) \times P(\overline{C} \mid I_E) \quad (2)$$

L'événement initiateur peut être décrit avec une probabilité sans dimension d'occurrence $P(I_E)$ ou avec une fréquence f_{IE} (1/fois). Si l'accent est placé sur le concept de fréquence, ce modèle mathématique peut également être utilisé pour calculer la fréquence $f\delta$ de la séquence δ dans l'Equation (3) avec la fréquence f_{IE} de l'événement initiateur:

$$f_\delta = f_{IE} \times P(A \mid I_E) \times P(\overline{B} \mid I_E) \times P(\overline{C} \mid I_E) \quad (3)$$

L'Equation (3) a été utilisée dans les exemples donnés en B.1.3, B.2.5 et B.2.6.

L'évaluation de toutes les séquences possibles α, β, γ, δ,…, ω donne une quantification exhaustive des conséquences de l'événement initiateur.

Si les données pour estimer l'occurrence de l'événement initiateur sont insuffisantes, il est recommandé de ne pas s'appuyer totalement sur la quantification, mais plutôt de recourir à l'analyse de sensibilité afin d'établir les séquences les plus critiques.

8.3.2 Liaison d'arbre de panne et réduction booléenne

Comme indiqué en 6.1 et compte tenu des limites de 5.2, les arbres de panne peuvent être utilisés pour calculer la probabilité conditionnelle des défaillances des facteurs d'atténuation.

La Figure 6 affiche un arbre d'événement avec deux facteurs d'atténuation, système A et système B. Les probabilités de défaillance des systèmes A et B sont respectivement indiquées par $P(F_A)$ et $P(F_B)$ et sont calculées en associant des arbres de panne qui, dans cette illustration uniquement, sont présentés avec leurs événements de tête comme conséquences à partir des portes ET ou OU, conformément à la CEI 61078 [16].

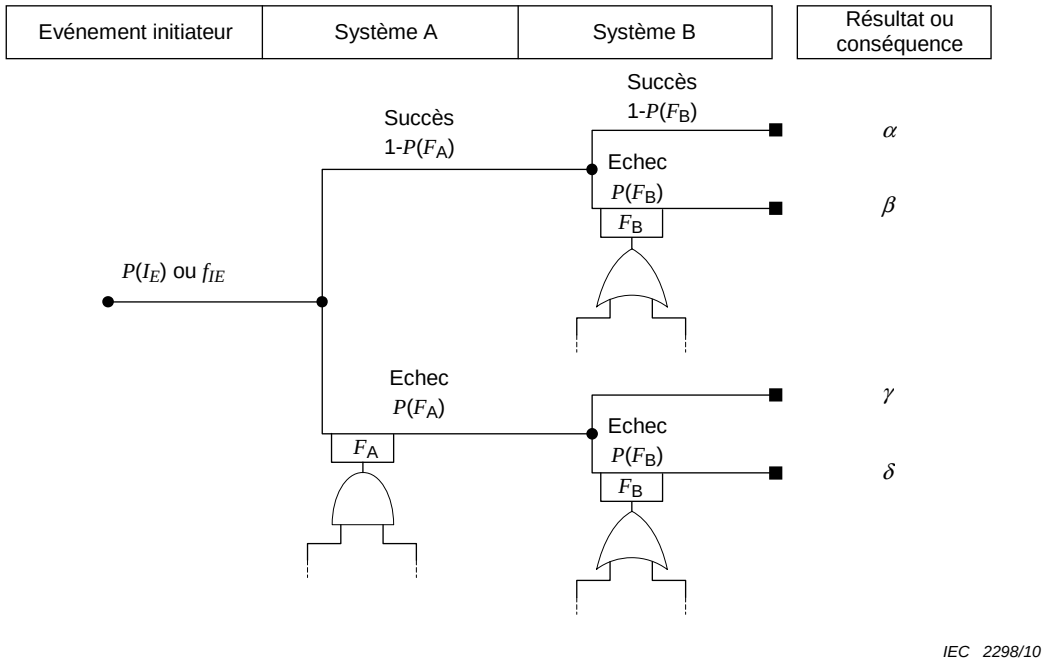

Figure 6 – Liaison d'arbre de panne

Les probabilités des événements de tête correspondant F_A et F_B font office de probabilités conditionnelles $P(F_A)$ et $P(F_B)$ pour la défaillance de système A et système B, respectivement. Les probabilités conditionnelles pour les succès des systèmes sont alors données par 1 – $P(F_A)$ et 1 – $P(F_B)$.

Lorsque les facteurs d'atténuation sont affectés par des événements de cause commune, l'algèbre booléenne peut être utilisée pour réduire l'arbre d'événement et identifier ces événements.

Les résultats de chaque séquence d'arbre d'événement sont réalisés en utilisant les concepts donnés dans [14]. La réduction booléenne nécessaire et l'analyse du premier impliquant sont réalisées conformément à [16].

L'Article B.3 donne un exemple détaillé de réduction booléenne et de premier impliquant pour un arbre d'événement spécifique.

Dans sa forme originale, l'événement de tête de l'arbre de panne lié aux différents facteurs d'atténuation génère une probabilité d'un état spécifique (succès, échec, par exemple) du facteur d'atténuation. Ces probabilités calculées par l'AAP peuvent être combinées à la probabilité d'occurrence ou de fréquence de l'événement initiateur (voir 8.3.1). Si l'occurrence de l'événement de tête est exprimée en termes de taux ou de fréquences de défaillance, ces mesures de l'occurrence de l'événement de tête ne peuvent pas être aisément combinées à la fréquence d'occurrence de l'événement initiateur. Par conséquent, il doit recourir à d'autres techniques d'analyse comme la modélisation de Markov (voir [17]). Si des stratégies de reprise ou de réparation non essentielles des différents facteurs d'atténuation sont impliquées, la modélisation de Markov peut faciliter la création d'un modèle plus réaliste. Pour une analyse plus détaillée des différents modes de fonctionnement d'un système et des mesures de sûreté de fonctionnement correspondantes, voir [18].

Des informations plus détaillées sur les fondements mathématiques du calcul par arbre d'événement sont disponibles en [32].

Les règles de base de la quantification se prêtent de manière relativement simple à une mise en œuvre informatique. La plupart des progiciels facilitent l'analyse qualitative et quantitative d'un arbre d'événement. Toutefois, la CEI ne conseille pas un progiciel particulier.

Des exemples pratiques illustrant les considérations théoriques de cet article sont donnés dans l'Annexe B.

Outre les aspects plus théoriques de la réorganisation, de l'extraction et des opérations booléennes de l'arbre de panne, il est important de définir des lignes directrices claires en matière d'objectifs et d'exigences de l'analyse. Une approche plus exhaustive permettant d'établir un mode opératoire concis d'AAE est proposée en [3].

9 Documentation

Il convient d'inclure certains éléments de base dans la documentation de l'AAE (voir ci-dessous). Des informations complémentaires et supplémentaires peuvent être fournies par souci de clarté, notamment dans le cas de systèmes complexes. Le point essentiel est que la documentation doit reprendre de manière exhaustive les étapes réalisées.

Ci-dessous, les articles entre parenthèses se rapportent à un exemple de l'Article B.2:

a) objectif et domaine d'application de l'analyse (B.2.2), (B.2.4);
b) description du système (B.2.3):
    1) description de la conception;
    2) fonctionnement du système;
    3) définitions détaillées des limites du système.
c) hypothèses (B.2.3), (B.2.4):
    1) hypothèses relatives à la conception du système;
    2) hypothèses de fonctionnement, de maintenance, d'essai et d'inspection;
    3) hypothèses de modélisation de la fiabilité et de la disponibilité.
d) AAE (B.2.5), (B.2.6):
    1) raison et sources de la liste des événements initiateurs;
    2) analyse, y compris la représentation graphique;
    3) sources des données utilisées.
e) résultats, conclusions et recommandations (B.2.7).

Pour obtenir des lignes directrices plus générales sur la documentation, voir [13].

Annexe A
(informative)

Représentation graphique

Une représentation graphique souvent utilisée d'un arbre d'événement est donnée dans la Figure A.1:

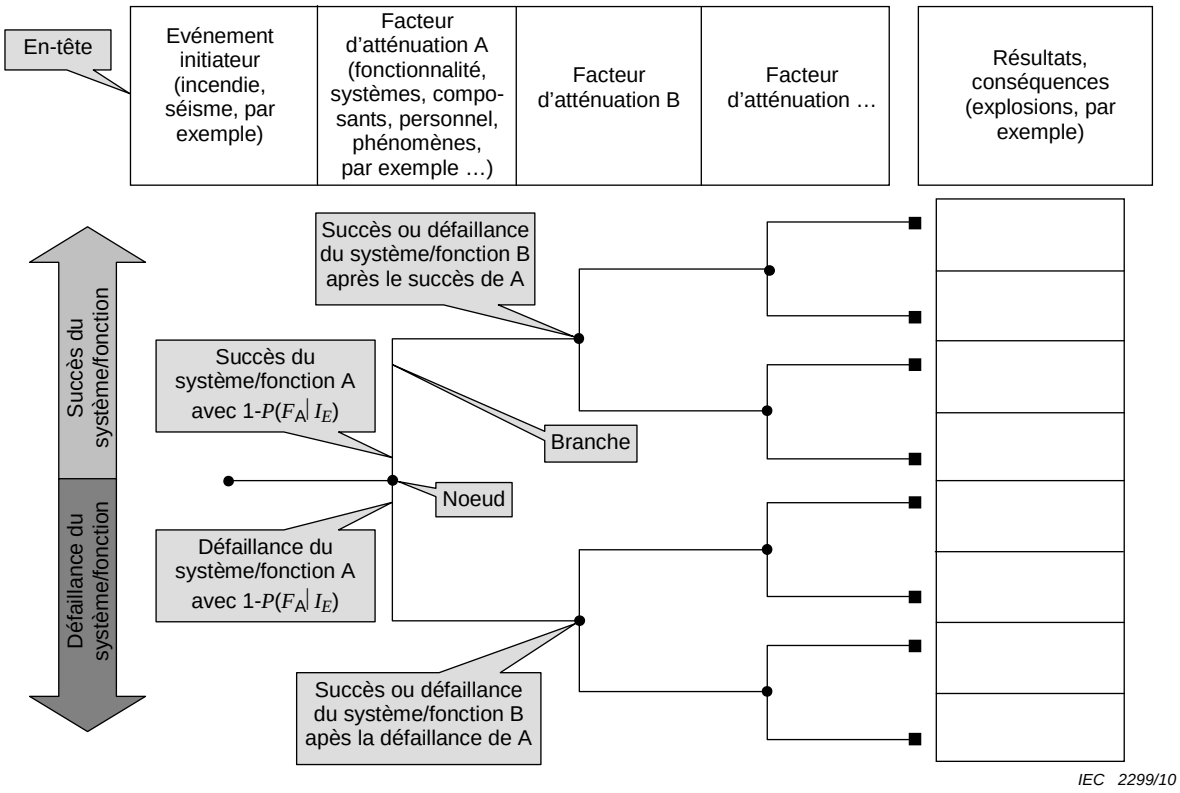

Figure A.1 – Représentation graphique souvent utilisée des arbres d'événement

Les explications nécessaires des éléments graphiques sont données dans le Tableau A.1:

Tableau A.1 – Éléments graphiques

Élément	Remarques
Branche	Voir 3.1.10 – Noter que deux branches ou plus peuvent partir d'un nœud. Pour plus de détails, voir également 7.2.5 c)1). Il convient de noter que les méthodes booléennes de l'Article B.3 s'appliquent uniquement dans le cas des branches binaires
En-tête	Voir 3.1.4
Événement initiateur	Voir 3.1.5
Facteur d'atténuation	Voir 3.1.6
Nœud	Voir 3.1.1
Résultat, conséquence	Voir 3.1.7
$P(F_{\mathrm{A}}\|I_{\mathrm{E}})$	Probabilité de la défaillance du facteur d'atténuation A dans les conditions dans lesquelles s'est produit l'événement initiateur (I_E)
Succès/échec	Afin de mettre en correspondance sans équivoque les conséquences possibles et le succès ou la défaillance du système ou de la fonction, il est indispensable d'établir des critères sans équivoque de succès ou de défaillance, respectivement

Annexe B
(informative)

Exemples

B.1 Incendie dans une centrale nucléaire

B.1.1 Vue d'ensemble

L'expérience au cours des quarante dernières années a montré que le risque provenant d'incendie dans une centrale nucléaire doit être pris en compte lorsque l'on analyse les facteurs contribuant au risque sévère d'un accident nucléaire sévère.

Voici un exemple d'analyse de risque de probabilité d'incendie avec un objectif double:

a) les zones critiques de la centrale qui présentent la plus importante contribution à la probabilité totale des principaux dommages de la centrale nucléaire doivent être identifiées par un processus de dépistage approprié; et

b) les séquences d'événements d'incendie doivent être établies. Elles reflètent les effets de la déclaration de l'incendie, de sa détection, de l'isolement de la salle, de la lutte contre l'incendie et des dommages aux équipements en raison de l'agent de suppression.

Dans une AAE quantitative, la fréquence des événements initiateurs provoqués par l'incendie et les différents dommages principaux doivent être déterminés.

Les tâches principales consistent à procéder à l'analyse quantitative et au processus de dépistage qualitatif afin d'identifier les emplacements critiques d'incendie, voir ce qui suit.

B.1.2 Analyse de dépistage

Dans la première étape, une collecte détaillée de données est réalisée dans toutes les salles de la centrale afin de les classer en fonction de leur importance et fonction. Les termes suivants sont des exemples issus d'une analyse spécifique.

Un secteur protégé contre les incendies est défini comme étant un bâtiment ou une partie d'un bâtiment, bien protégé par des coupe-feux empêchant la propagation aux bâtiments ou parties de bâtiment adjacents.

Un compartiment d'incendie est une subdivision d'un secteur protégé contre les incendies visant à s'assurer que les conséquences indésirables d'un incendie ne se propagent pas aux autres subdivisions.

Un compartiment d'incendie essentiel contient les équipements liés au fonctionnement en régime de puissance, les équipements liés à la sécurité ou les combustibles stockés de manière fixe ou temporaire.

Un compartiment d'incendie critique est un compartiment d'incendie essentiel dans lequel un incendie peut endommager au moins un composant ou système de sécurité et déclencher un événement initiateur de sécurité dans la centrale nucléaire.

Le processus de dépistage commence par l'identification de toutes les salles pour lesquelles l'un au moins des trois critères ci-dessous est respecté:

a) charge calorifique >7 kWh/m^2;

b) la salle contient des équipements de sécurité ou leurs câbles;

c) la salle contient des équipements d'exploitation ou de détection du système de protection du réacteur (système de commande de sécurité).

Les salles pour lesquelles les trois critères sont respectés simultanément sont identifiées comme des compartiments d'incendie essentiels.

B.1.3 Analyse quantitative

Pour chaque compartiment d'incendie critique, un arbre d'événement est développé avec un nœud pour la déclaration d'incendie, la ventilation de la salle, la détection de l'incendie, la lutte contre l'incendie et la propagation. Tous les facteurs d'atténuation de l'arbre d'événement sont considérés comme indépendants les uns des autres (voir les limites en 5.2). La Figure B.1 illustre un arbre d'événement classique pour un feu d'hydrocarbure dans la salle d'un générateur diesel.

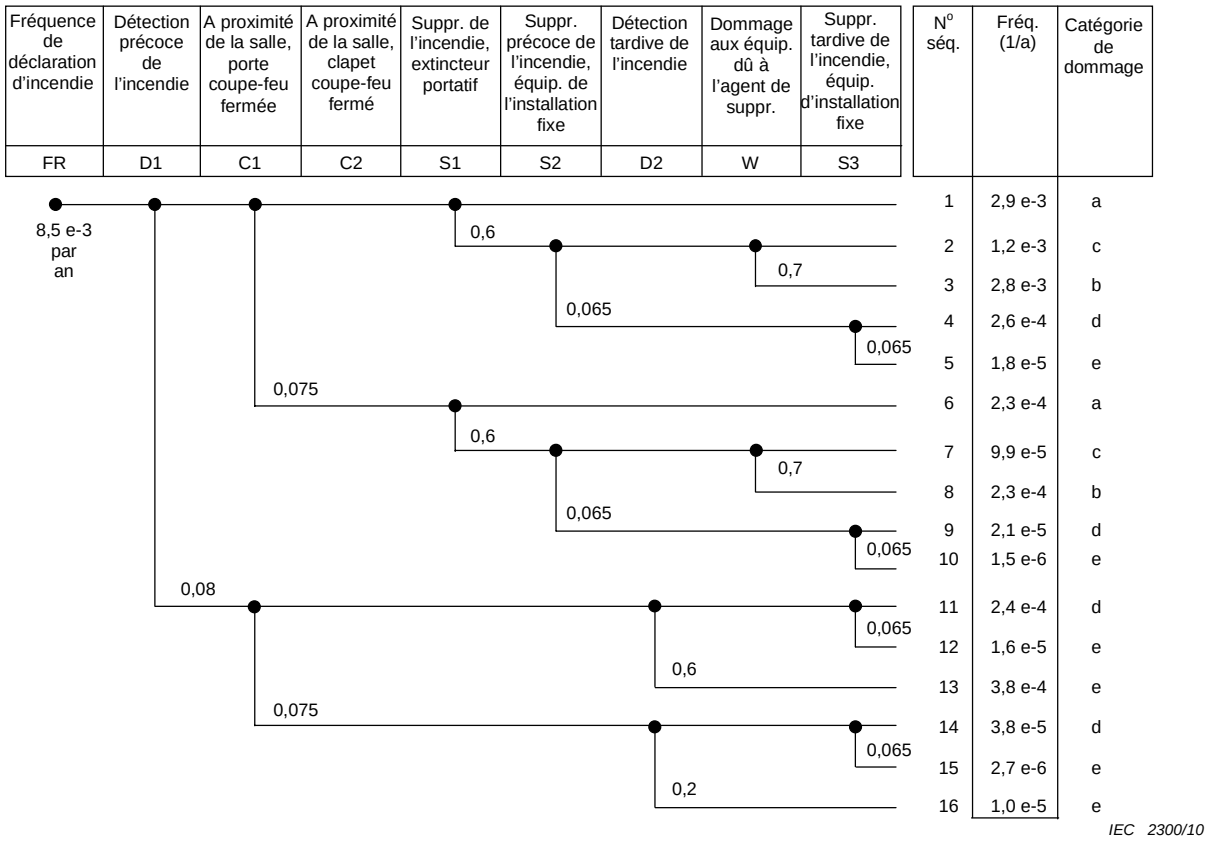

Figure B.1 – Arbre d'événement d'un incendie classique dans un bâtiment de générateur diesel

On doit utiliser des données appropriées pour la fréquence de déclaration d'incendie et les différents nœuds. Autant que possible, il convient que ces données soient spécifiques à la centrale. Toutefois, en l'absence de données spécifiques à la centrale, des données de base internationales telles que les dernières publiées relatives aux centrales américaines peuvent être utilisées. Pour calculer la fréquence d'incendie d'une salle individuelle dans un bâtiment, des facteurs de pondération supplémentaires reposant sur la quantité de sources d'inflammation, le poids de l'isolation du câble, le nombre de zones d'incendie pertinentes et des facteurs particuliers des sources d'inflammation sont requis.

Les conséquences sont classées en cinq catégories de dommages (a), (b), (c), (d) et (e), la pire catégorie étant définie comme (e) « Dommage et propagation complets ». Cela se produit lorsque toutes les mesures de protection incendie n'ont pas permis d'empêcher la propagation aux salles adjacentes. Tous les équipements de sécurité des salles voisines sont endommagés.

Pour chaque compartiment d'incendie critique, les résultats suivants sont obtenus:

a) fréquence et nature des transitoires générés par l'incendie dans la centrale nucléaire;

b) une liste des équipements endommagés classés en fonction de la catégorie de dommage (a) – e);

c) fréquence des catégories de dommage.

La Figure B.2 illustre une version simplifiée d'un arbre d'événement. La fréquence d'un incendie généralisé déclenché par un feu naissant et l'indisponibilité ou défaillance résultante de la détection incendie sont déduites en multipliant la fréquence de l'événement initiateur de 1,0e-4 par année par la probabilité de l'indisponibilité de la détection incendie de 1,0e-3 par année. Ceci donne une fréquence résultante de 1,0e-7 par année de l'événement indésirable d'un incendie généralisé.

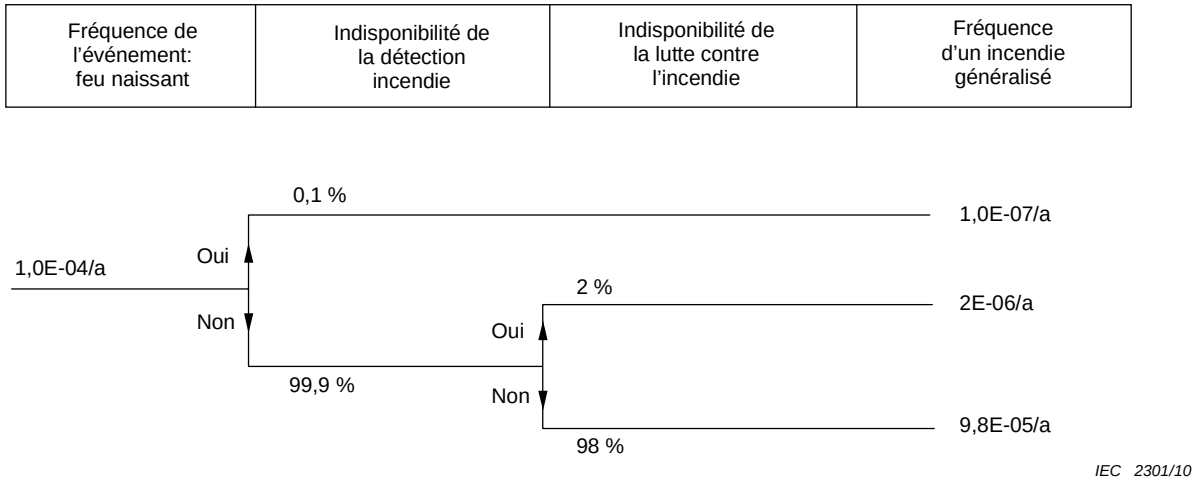

Figure B.2 – Arbre d'événement simplifié en cas d'incendie

B.1.4 Résultats

L'AAE est un excellent outil de classement, d'évaluation et de présentation des dysfonctionnements possibles. Elle permet de définir les priorités en matière de mesures d'amélioration de la protection incendie. Des études supplémentaires des coûts/avantages peuvent s'appuyer sur les résultats obtenus.

B.2 AAE appliquée à un passage à niveau

B.2.1 Symboles et acronymes

Les symboles du Tableau B.1 ci-dessous sont utilisés dans la présente annexe:

Tableau B.1 – Symboles utilisés dans l'Annexe B

Symbole	Description
A_k	Scénario d'accident k
C_k	Probabilité de conséquence
D	Durée du danger
E	Exposition totale par utilisation
F_k	Probabilité d'accident mortel
IRF	Risque individuel d'accident mortel (*individual risk of fatality*)
H	Danger
HR	Taux de défaillance (*hazard rate*) (au sens de « taux de défaillance instantané » de la CEI 61703:2001, 6.1.3) [20])
k	Nombre de scénarii différents
LX	Passage à niveau
N	Nombre d'utilisations du passage à niveau par an et par personne
THR	Taux de défaillance tolérable (*tolerable hazard rate*) (au sens de « taux de défaillance instantané » de la CEI 61703:2001, 6.1.3 [20])
P_C	Probabilité de « collision avec un train »
P_{EA}	Probabilité « d'impossibilité à éviter » (*probability of unable to to take evasive action)*
P_N	Probabilité « d'absence de signalisation opportune du train »
P_{Tr}	Probabilité « d'approche du train »
TIR	Cible du niveau de risque acceptable individuel (*Target for the Individual acceptable level of Risk)*

B.2.2 Objectif

Afin d'illustrer l'application de l'AAE, l'Article B.2 donne un exemple de répartition "orientée risque" des exigences en matière d'intégrité de sécurité d'un système de signalisation de chemins de fer, à savoir un passage à niveau.

L'analyse consiste à déduire les objectifs de sécurité d'un événement initiateur défini en tenant compte de toutes les conditions opérationnelles, environnementales et architecturales. Cet objectif est atteint au moyen d'une AAE « inversée » (voir B.2.6). Dans ce contexte, l'arbre d'événement « inversé » consiste à déduire la fréquence tolérable de l'événement initiateur par inversion du mode de calcul, en commençant par les conséquences.

Ni la fonctionnalité ni l'analyse ne ressemblent directement aux fonctions d'un type particulier de passage à niveau. L'objectif principal est de présenter un exemple de méthodologie plutôt que de proposer une analyse réaliste détaillée. En particulier, les valeurs utilisées dans les calculs sont des exemples qu'il convient de ne pas considérer comme étant factuelles.

B.2.3 Définition du système

L'exemple ci-dessous d'un système de signalisation de chemins de fer (passage à niveau automatique) a fait l'objet de nombreuses analyses.

Dans cet exemple, le passage à niveau automatique a été exploité pendant 25 ans. Il est équipé de signaux lumineux à l'attention des usagers de la route, et d'un signal distant (surveillance) pour informer le conducteur de train de la fermeture ou de l'ouverture du passage à niveau.

Un schéma du passage à niveau (LX) est donné dans la Figure B.3**.**

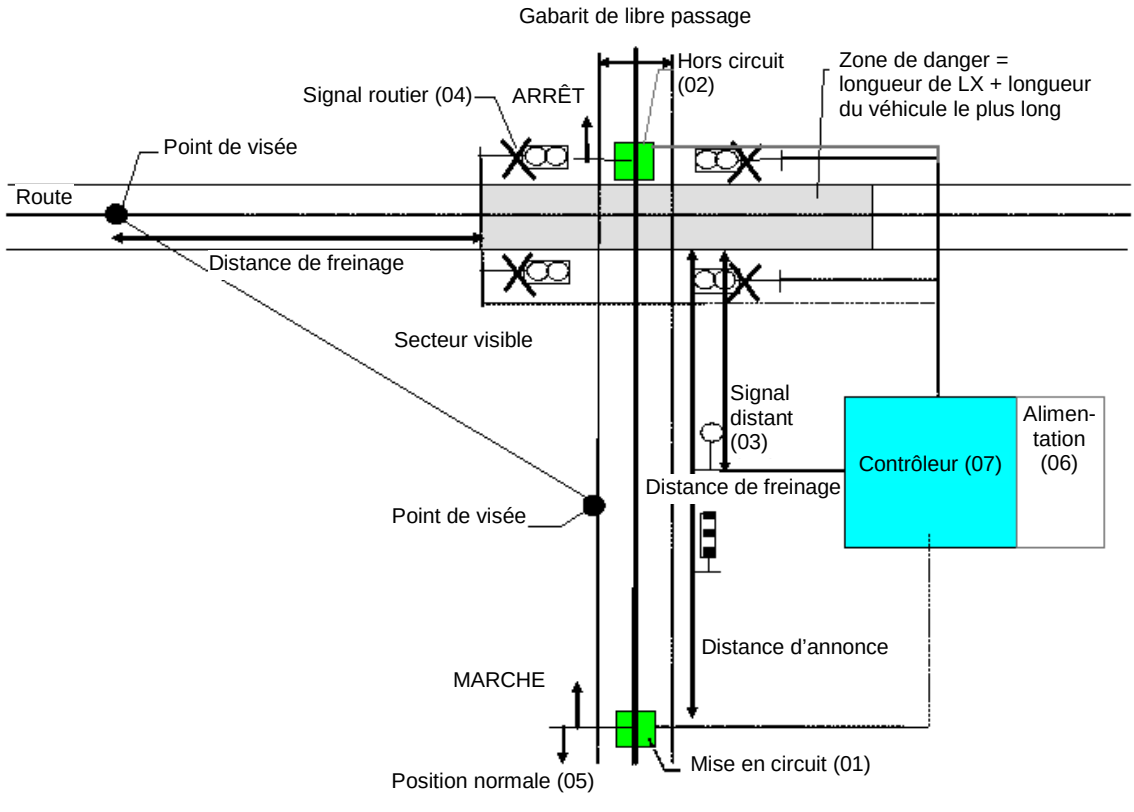

Figure B.3 – Système de passage à niveau (LX)

Étant donné que la définition complète du système n'entre pas dans le domaine d'application de cet exemple, seule une description fonctionnelle informelle est donnée ici. Le Tableau B.2 présente les principales unités fonctionnelles concernées.

Tableau B.2 – Présentation du système

N°	Unité fonctionnelle	Remarques
01	Mise en circuit du passage à niveau	Déclenche l'activation du passage à niveau à l'approche d'un train, au moyen d'un équipement de détection de roue (un compteur d'essieux, par exemple)
02	Mise hors circuit du passage à niveau	Déclenche la désactivation du passage à niveau après le passage du train, au moyen d'un équipement de détection de roue (un compteur d'essieux, par exemple)
03	Surveillance du passage à niveau	Affiche l'état du passage à niveau au conducteur de train ou au système d'enclenchement (mis en œuvre, par exemple, au moyen d'un signal distant) afin de surveiller le fonctionnement du passage à niveau
04	Signalisation routière	Affiche l'état du passage à niveau aux usagers de la route
05	Position normale	Replace le passage à niveau en position normale (sans protection) s'il a été mis en route, mais qu'il n'a pas été arrêté dans un certain laps de temps (en raison, par exemple, d'une défaillance du capteur qui signale toujours la présence d'un train alors qu'il a déjà quitté le passage à niveau ou si le train s'est arrêté avant le passage à niveau, etc.)
06	Alimentation	Comprend un système d'alimentation normal ou une batterie de secours capable de faire fonctionner le passage à niveau pendant une période limitée (2 h, par exemple). La tension de la batterie est surveillée à distance par le système d'enclenchement
07	Contrôle	Active et contrôle le passage à niveau. Un dispositif électronique programmable contenant un logiciel d'application, des données spécifiques au site, etc.

Une description concise de l'arbre de panne du passage à niveau est donnée dans l'énumération ci-dessous:

a) Un train à l'approche est détecté par l'élément de mise en route (01) et signalé au contrôleur (07). La distance entre l'élément de mise en route (01) et le passage à niveau est désignée "distance d'annonce".

b) Le contrôleur commande d'activer les signaux routiers (04) et attend la confirmation de réception de la position de mise en circuit. La distance entre le point de visée et le passage à niveau est désignée "distance de freinage".

c) Le contrôleur commande d'activer le signal distant (03), représenté par un petit cercle sur une petite ligne verticale perpendiculaire à une petite ligne horizontale. La position par défaut est « arrêt » (danger). Si le signal distant est « arrêt », un train à l'approche doit s'arrêter au passage à niveau, que le conducteur peut mettre en route manuellement à l'aide d'une clé en mode de secours.

d) Un élément de mise hors circuit (02) détecte la traversée du passage à niveau par le train et en informe le contrôleur.

e) Le contrôleur commande de désactiver le signal distant. Après un certain laps de temps, les signaux routiers sont mis hors circuit.

B.2.4 Identification des dangers

Dans le secteur ferroviaire, les événements initiateurs au niveau du système sont classés comme des dangers conformes aux normes CENELEC pertinentes.

Une analyse exhaustive des dangers possibles n'est pas réalisée. Seul le danger H indiqué ci-dessous est pris en compte.

H = Inaptitude du passage à niveau à protéger les personnes du train

Ce danger est censé couvrir toutes les situations dans lesquelles il convient que le passage à niveau signale l'approche d'un train au public, ce qui n'est pas le cas.

L'objectif est de déterminer le taux de défaillance HR (1/fois) de H acceptable en fonction de certains critères d'acceptation des risques. Le terme « taux » est utilisé au sens de « taux de défaillance instantané » tel qu'il est décrit en 6.1.3 de la CEI 61703 :2001 [20].

B.2.5 AAE

Afin de déterminer les conséquences possibles du danger H, examiner les scénarii dans lesquels un individu fait face à ce danger, dans le cas particulier, par exemple, d'un automobiliste approchant d'un passage à niveau non protégé. Dans cet exemple, P_{TR} désigne la probabilité de l'absence d'un train à l'approche, P_N la probabilité de signalisation opportune du train par le conducteur, P_{EA} la probabilité d'un évitement, et P_C la probabilité d'une collision réelle avec le train.

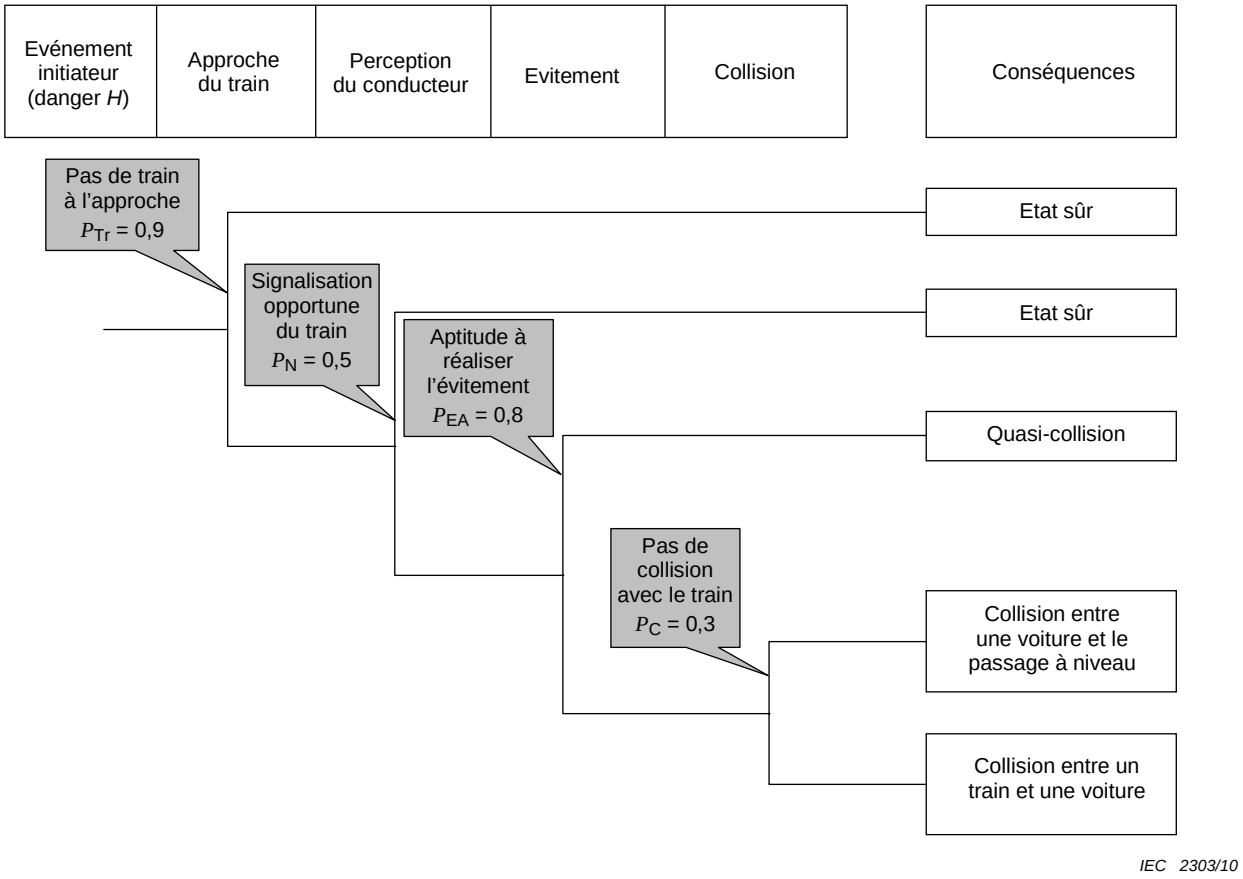

Figure B.4 – AAE d'un système de passage à niveau

Par conséquent, deux types d'accidents (« Collision entre un train et une voiture » et « Collision entre une voiture et un passage à niveau ») sont identifiés. La Figure B.4 illustre les facteurs de réduction des risques externes (c'est-à-dire les facteurs d'atténuation, voir 3.1.6) entre l'événement initiateur (c'est-à-dire le danger) et les conséquences (c'est-à-dire les accidents).

B.2.6 Analyse quantitative

NOTE Compte tenu des limites de 5.2, l'analyse quantitative suivante met l'accent sur des résultats conservatoires.

Les figures de référence de Railtrack's Railway Group Safety Plan (1997/98) [33] sont considérées comme les cibles du niveau individuel acceptable du risque (TIR) d'un automobiliste: « La mise en œuvre des projets raisonnablement réalisables se poursuit, avec pour objectif d'assurer que les passages à niveau automatiques n'exposent pas les usagers de la route à un risque d'accident mortel supérieur à un sur 100 000 usagers réguliers par an en 2000 ».

Afin de définir une limite largement acceptable, un facteur de sécurité supplémentaire de 10 est ajouté. En d'autres termes, il convient que le risque individuel déduit de $R_i < 10^{-5}$ accidents mortels/(personne × année) pour un utilisateur régulier soit inférieur à 10^{-6} par an. Par conséquent, la valeur TIR est établie à moins de 10^{-6} par an.

Afin d'obtenir l'approbation des autorités, l'entreprise de chemin de fer doit démontrer que le Risque Individuel d'Accident Mortel (IRF) réel est inférieur ou égal à la valeur TIR. La déduction suivante du taux de danger acceptable repose sur l'équation de IRF issu de [4]. Ce modèle mathématique de détermination du risque individuel tient compte des liens de causalité entre l'événement initiateur (c'est-à-dire les dangers) et les conséquences (c'est-à-dire les séquences d'accidents).

a) Il est supposé qu'un individu utilise le passage à niveau avec un profil d'utilisation décrit par le nombre d'utilisation N (par an). Pour référence, une exposition totale par utilisation E peut être définie (E étant le temps nécessaire à la traversée d'un passage à niveau).

b) Dans cet exemple, l'individu est exposé au danger H. En outre, la probabilité d'exposition de cet individu au danger dépend de la durée du danger D et de la durée d'exposition E de l'individu aux dangers. Cette probabilité est la somme des probabilités que le danger existe déjà lorsque l'individu entre dans le système (environ HR x D) et de la probabilité selon laquelle le danger se produira pendant l'exposition de l'individu (environ HR x E).

c) De chaque danger peut résulter un ou plusieurs types de séquences d'accidents. Cela est décrit pour chaque danger par la probabilité de conséquence C_k qu'un accident A_k se produise. Cette probabilité représente les facteurs externes de réduction du risque (c'est-à-dire les facteurs d'atténuation, voir 3.1.6) obtenus par l'AAE (Figure B.4). A chaque type associé d'accident A_k, correspond une gravité qui, au niveau de l'individu, est décrite comme la probabilité d'accident mortel F_k pour un seul individu (Tableau B.3). A titre d'exemple, la gravité de l'accident a été estimée et comparée avec les données de chemin de fer [33].

Tableau B.3 – Paramètres de réduction des risques pour les accidents de la Figure B.4

N° *k*	Accident A_k	Facteur de réduction des risques C_k	Probabilité d'accident mortel F_k
1	Collision entre un train et une voiture	0,1×0,5×0,2×0,7 = 0,007	0,2
2	Collision entre une voiture et un passage à niveau	0,1×0,5×0,2×0,3 = 0,003	0,05

Cela donne lieu à un risque individuel d'accident mortel défini par

$$\text{IRF} = \text{N} \times H_{\text{R}} \times (D + E) \times \sum_{\text{accidents } A_k} (C_k \times F_k) \qquad \text{(B.1)}$$

L'Equation (B.1) peut être évaluée à l'aide de valeurs moyennes ou en insérant des paramètres appropriés (des pourcentages, par exemple) de répartitions statistiques pour les paramètres d'entrée.

Si le risque individuel s'avère moindre que le risque individuel cible, le taux de défaillance (HR) calculé ou estimé est appelé taux de défaillance tolérable (THR).

Pour les besoins de cet exemple, il est considéré qu'un automobiliste traverse une voie de chemin de fer de manière répétée, N = 1 000 fois par an. Les autres usagers (les piétons ou les cyclistes, par exemple) ne sont pas pris en compte.

Selon l'expérience en exploitation, il est supposé que le danger H, s'il se produit, dure beaucoup plus longtemps que la durée d'exposition individuelle, qui serait la durée de traversée du passage à niveau. Cela signifie qu'il est possible d'ignorer la durée d'exposition individuelle E de l'Equation (B.1). La valeur pessimiste de la durée du danger D = 10 h est prise pour hypothèse. Il s'agit de la durée de défaillance du passage à niveau qui donne lieu à un état dangereux du système (tant qu'il n'est pas inversé ou réparé).

Le taux de défaillance tolérable (THR) de H peut être calculé en insérant les paramètres dans l'Equation (B.2), comme suit:

$$\begin{aligned} \text{IRF} &= \text{N} \times H_{\text{R}} \times (D + E) \times \sum_{\text{accidents } A_k} (C_k \times F_k) \\ &= 1000 \times \text{HR} \times 10 \times (0{,}007 \times 0{,}2 + 0{,}003 \times 0{,}05) \\ &\leq \text{TIR} = 10^{-6} \text{ par an} \end{aligned} \tag{B.2}$$

Cela donne un taux tolérable d'occurrence de l'événement initiateur (c'est-à-dire le danger) d'environ $7 \times 10^{-8}\ \text{h}^{-1}$, soit environ un danger tolérable d'inaptitude du passage à niveau à protéger les personnes du train tous les 1 600 ans.

B.2.7 Analyse des conséquences et définition de l'action nécessaire

A l'issue de l'analyse, il revient au concepteur ou au fabricant du passage à niveau de déterminer si son système peut atteindre le taux de défaillance tolérable ou s'il s'avère nécessaire d'apporter des modifications d'ordre architectural ou conceptuel de manière à atteindre les cibles quantitatives.

B.2.8 Conclusion

Cet exemple de signalisation de chemin de fer a illustré une autre approche de l'AAE dans laquelle il est possible d'utiliser une approche inversée déduisant les taux tolérables de l'événement initiateur des conséquences observées à l'aide des paramètres de réduction des risques.

B.3 Liaison d'arbre de panne et réduction booléenne

NOTE Cet article propose des concepts théoriques qui sont à la base des progiciels les plus souvent utilisés pour la réduction booléenne. Il convient que le lecteur comprenne les algorithmes de base de manière à bien appréhender la technique. En outre, cette approche s'applique aux arbres d'événement avec des branches binaires uniquement.

Lorsque différents facteurs d'atténuation partagent un facteur de cause commune, l'algèbre booléenne peut permettre d'identifier ces causes communes lors de l'évaluation qualitative de l'arbre d'événement. Les « premiers impliquants » résultant de l'analyse qualitative sont alors utilisés pour la quantification de la fréquence d'une conséquence spécifique.

En fait, chaque conséquence est obtenue en combinant, à l'aide d'une porte logique ET, les événements de tête des arbres de panne liés (voir 8.3.2) associés à la défaillance des facteurs d'atténuation. De même, les « premiers impliquants » de ce nouvel arbre logique sont recherchés.

Les séquences minimales sont la plus petite combinaison d'événements résultant des conséquences inacceptables. Il s'agit, en réalité, d'une instance spéciale des« premiers impliquants ». Si l'arbre de panne est cohérent (s'il contient uniquement des portes ET

et OU), il est possible de remplacer la notion de « premiers impliquants » par « séquences minimales ». Pour de plus amples informations sur la théorie des « premiers impliquants » et des séquences minimales, voir [38].

Les « premiers impliquants » sont identifiés pour l'événement résultant d'une combinaison de portes ET des événements uniquement liés aux défaillances des facteurs d'atténuation. Un exemple de réduction booléenne d'un arbre d'événement est présenté dans la Figure B.5.

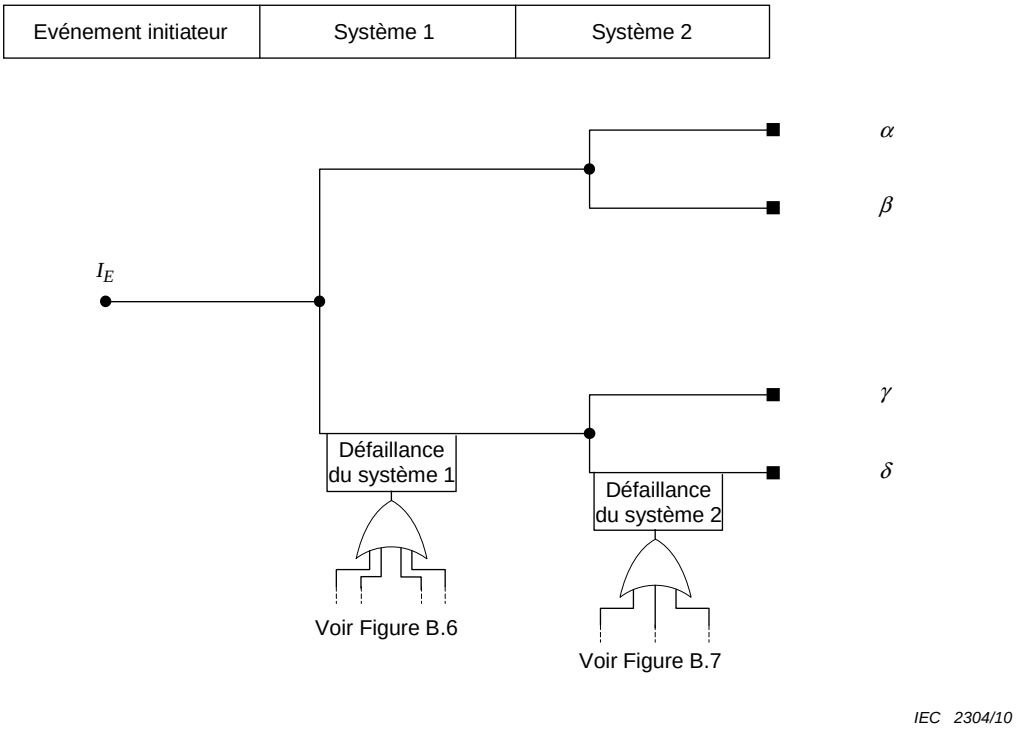

Figure B.5 – Exemple simple

Les probabilités de défaillance des systèmes 1 et 2 peuvent être modélisées par la liaison d'arbre de panne comme décrit en 8.3.2.

Les arbres de panne théoriques ci-dessous représentent la structure logique de la défaillance du système 1 (voir Figure B.6) et du système 2 (voir Figure B.7), respectivement, impliquant sept événements de base A, B, C, D, E, F et G. Les symboles sont utilisés conformément à la CEI 61078 [16].

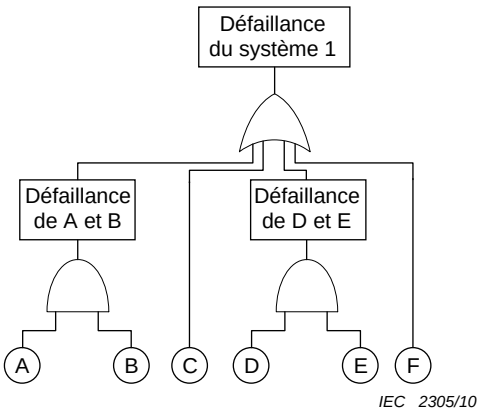

Figure B.6 – Arbre de panne pour la défaillance du système 1

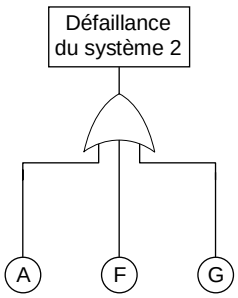

Figure B.7 – Arbre de panne pour la défaillance du système 2

Avec ces arbres de panne et l'arbre d'événement, les expressions booléennes réduites pour les conséquences $\alpha, \beta, \gamma, \delta$ sont les suivantes:

$$\alpha = I_E.\left(\overline{A}.\overline{C}.\overline{D}.\overline{F}.\overline{G} + \overline{A}.\overline{C}.\overline{E}.\overline{F}.\overline{G}\right) \quad \text{(B.3)}$$

$$\begin{aligned}\beta = I_E.(&A.\overline{B}.\overline{C}.\overline{D}.\overline{F} + A.\overline{B}.\overline{C}.\overline{E}.\overline{F} + \\ &+ \overline{A}.\overline{C}.\overline{D}.\overline{F}.G + \overline{A}.\overline{C}.\overline{E}.\overline{F}.G + \\ &+ \overline{B}.\overline{C}.\overline{D}.\overline{F}.G + \overline{B}.\overline{C}.\overline{E}.\overline{F}.G)\end{aligned} \quad \text{(B.4)}$$

$$\gamma = I_E.\left(\overline{A}.C.\overline{F}.\overline{G} + \overline{A}.D.E.\overline{F}.\overline{G}\right) \quad \text{(B.5)}$$

$$\delta = I_E.\left(F + A.B + A.C + G.C + A.D.E + G.D.E\right) \quad \text{(B.6)}$$

Si δ est la conséquence à analyser, les premiers impliquant sont

$$I_E.F, \quad I_E.A.B, \quad I_E.A.C, \quad I_E.G.C, \quad I_E.A.D.E, \quad I_E.G.D.E$$

Les événements de base A et F sont communs aux deux arbres de panne. Conformément à 8.2.3, ils peuvent être extraits (pour donner Système 1* (S_1^*) et Système 2* (S_2^*) sans A et F) et introduits comme nouveaux facteurs d'atténuation dans un nouvel arbre d'événement (voir Figure B.8).

Noter que dans cet exemple particulier, A et F utilisés dans un environnement d'arbre de panne illustraient l'occurrence des événements donnant lieu à une défaillance des systèmes (Figures B.6 et B.7). Par conséquent, la branche supérieure représente un développement vers la défaillance du système.

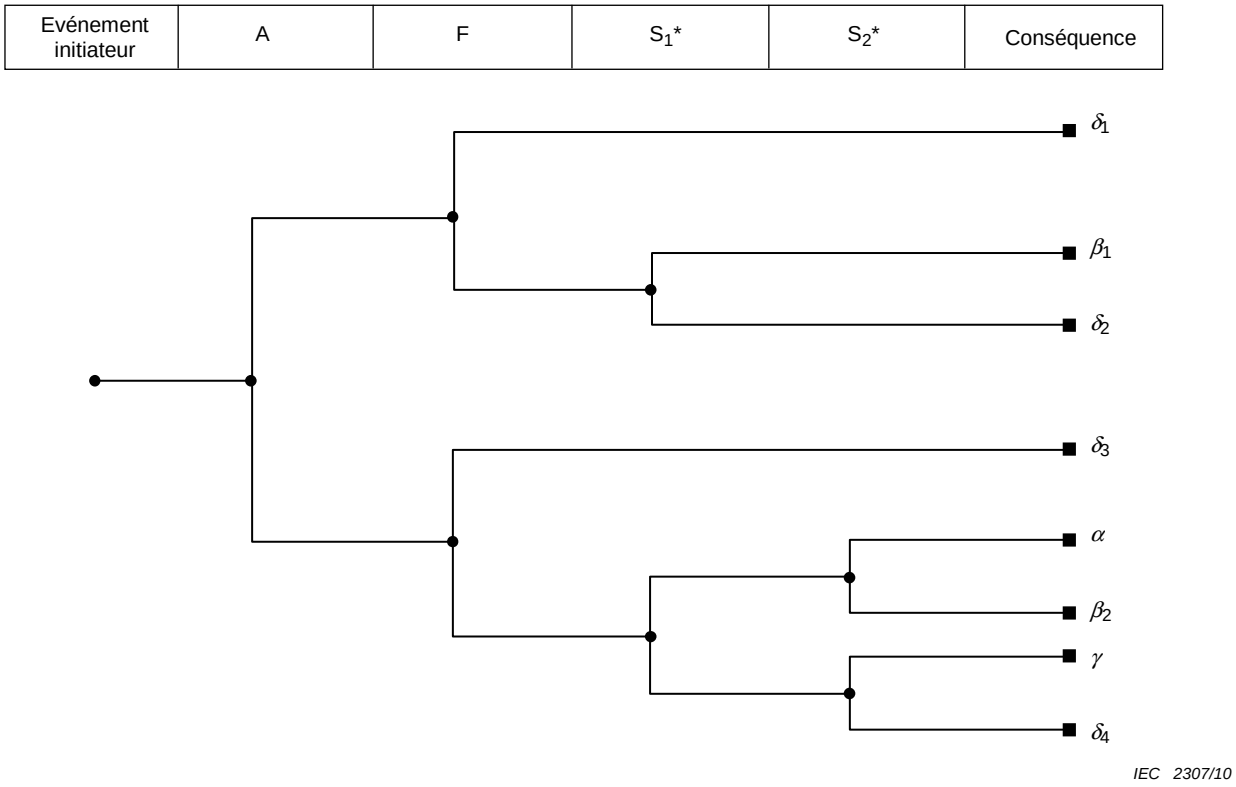

Figure B.8 – Arbre d'événement modifié

L'équivalence entre ces deux schémas de principe et les égalités suivantes peut être vérifiée (voir [16]):

$$\beta = \beta_1 + \beta_2 \qquad \text{(B.1)}$$

ainsi que

$$\delta = \delta_1 + \delta_2 + \delta_3 + \delta_4 \qquad \text{(B.2)}$$

avec

$$\beta_1 = I_E.\left(A.\overline{F}\,.\,S_1^*\right),$$

$$\beta_2 = I_E.\left(\overline{A}.\overline{F}\,.\,S_1^*.\,\overline{S}_2^*\right),$$

$$\delta_1 = I_E.\left(A.\,F\right),$$

$$\delta_2 = I_E.\left(A.\,\overline{F}\,.\,\overline{S}_1^*\right),$$

$$\delta_3 = I_E.\left(\overline{A}\,.\,F\right), \text{ et}$$

$$\delta_4 = I_E.\left(\overline{A}.\,\overline{F}\,.\,\overline{S}_1^*.\,\overline{S}_2^*\right).$$

Les « pannes globales groupées" suivantes peuvent être examinées:

« Perte du système 1 »:

$$G_1 = D.E + C \tag{B.3}$$

« Perte du système 2 »:

$$G_2 = A + G \tag{B.4}$$

« Perte des systèmes 1 et 2 »:

$$G_3 = F + A.B \tag{B.5}$$

L'arbre d'événement suppose le format suivant:

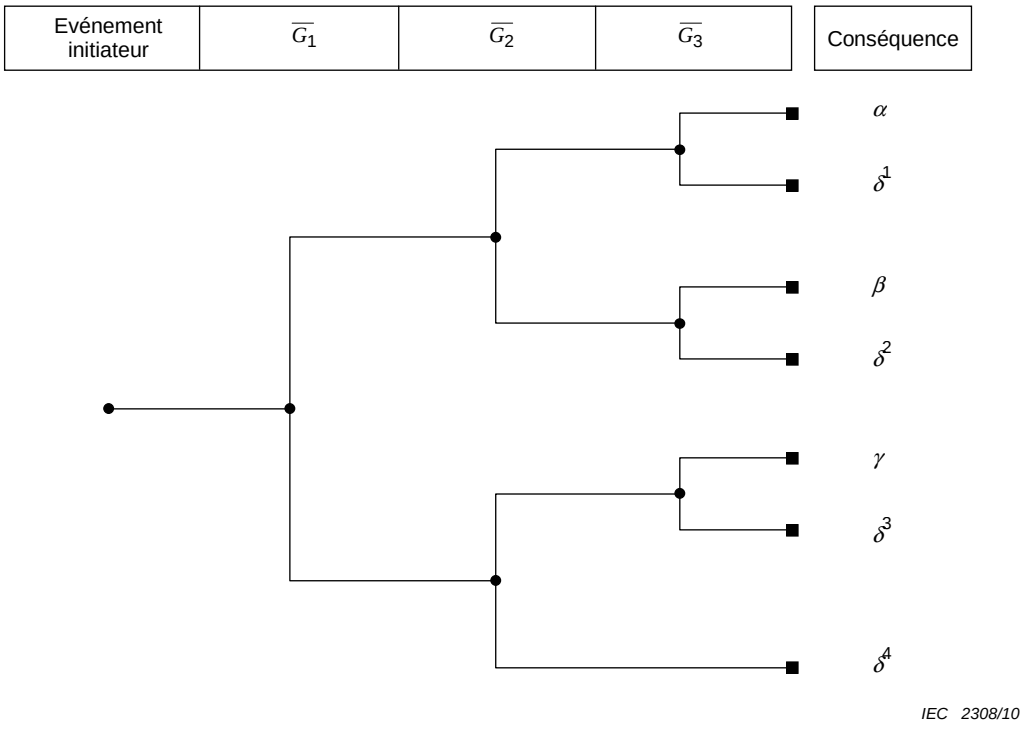

Figure B.9 – Arbre d'événement avec « pannes groupées »

L'équivalence entre ces schémas de principe et l'égalité suivante peut être vérifiée (voir la CEI 61078 [16]):

$$\delta = \delta^1 + \delta^2 + \delta^3 + \delta^4 \tag{B.6}$$

avec

$$\delta^1 = \overline{G_1} \,.\, \overline{G_2} \,.\, G_3 \,,$$

$$\delta^2 = \overline{G_1} \,.\, G_2 \,.\, G_3 \,,$$

$$\delta^3 = G_1 \,.\, \overline{G_2} \,.\, G_3 \,, \text{ et}$$

$$\delta^4 = G_1 \,.\, G_2 \ .$$

Une approche plus approfondie de l'analyse booléenne, y compris des conseils détaillés sur les méthodes de disjonction, sont disponibles dans la CEI 61078 [16].

Bibliographie

[1] American Institute of Chemical Engineers, *Layer of Protection Analysis – Simplified process risk assessment*, New York, USA, October 2001

[2] ANDREWS, J.D., DUNNETT, S.J. *Event Tree Analysis using Binary Decision Diagrams*, IEEE Trans. Reliability, Vol 49, pp 230 – 238, 2000

[3] ASME Standard for *Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME RA-S-2002, 2002, Amended by addenda ASME RA-Sa-2003, ASME RA-Sb 2005, and ASME RA-Sc-2007

[4] BRABAND, J., LENNARTZ, K. *A Systematic Process for the Definition of Safety Targets for Railway Signalling Applications*, Signal+Draht, 9/99

[5] DOWELL, III, A.M., HENDERSHOT, D.C, *Simplified Risk Analysis – Layer of Protection Analysis (LOPA)*, American Institute of Chemical Engineers, Indianapolis, 2002

[6] Expert Group on Probabilistic Safety Analysis for Nuclear Power Plants, "*Methods for Probabilistic Safety Analysis for Nuclear Power Plants, Status: August 2005*", BfS-SCHR-37/05, Salzgitter, October 2005 (In German)

[7] FULLWOOD, R., HALL, R. *Probabilistic Risk Assessment in the Nuclear Power Industry*, New York, 1988

[8] GOLDBERG, B.E., EVERHART, K., STEVENS, R., BABBITT III, N., CLEMENS,P., STOUT, L. *System Engineering "Toolbox" for Design-Oriented Engineers*, NASA Reference Publication 1358, 1994

[9] *Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, NRC 1998.

[10] HENLEY, E.J., KUMAMOTO, H. *Reliability Engineering and Risk Assessment*, 1981

[11] HOFER, E., KLOOS, M., KRZYKACZ-HAUSMANN, B., PESCHKE, J., SONNENKALB, M. *Dynamic Event Trees for Probabilistic Safety Analysis, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS)*, Proceedings EUROSAFE, Berlin 4-5 November 2002

[12] ISO/CEI 31010, *Management du risque — Lignes directrices pour l'évaluation du risque*

[13] CEI 60300-3-1:2003, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*

[14] CEI 60300-3-9,1995, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques*

[15] CEI 60812:2006, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

[16] CEI 61078:2006, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

[17] CEI 61165:2006, *Application des techniques de Markov*

[18] CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*

[19] CEI 61511-3:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

[20] CEI 61703:2001, *Expressions mathématiques pour les termes de fiabilité, de disponibilité, de maintenabilité et de logistique de maintenance*

[21] CEI 62425:2007, *Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement – Systèmes électroniques de sécurité pour la signalisation*

[22] CEI 62429:2007, *Croissance de fiabilité – Essais de contraintes pour révéler les défaillances précoces d'un système complexe et unique*

[23] IEC 62508:2010, *Guidance on human aspects of dependability* (disponible uniquement en anglais)

[24] CEI 62551, *Techniques d'analyse pour la sûreté de fonctionnement – Modélisation par réseau de Petri* [3]

[25] ISO 3534-1:2006, *Statistique – Vocabulaire et symboles – Partie 1: Termes statistiques généraux et termes utilisés en calcul des probabilités*

[26] KLOOS, M., PESCHKE, J. MCDET: *A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach, Nuclear Science and Engineering*: 153, 137-156, 2006

[27] LEVESON, N.G. SAFEWARE: *System Safety and Computers*, Addison-Wesley Publishing Company, 1995

[28] McCORMICK, N.J. *Reliability and Risk Analysis – Methods and Nuclear Power Applications*, Boston, 1981

[29] Nuclear Regulatory Commission, PRA Procedures Guide, *A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, Final Report, NUREG/CR-2300 Vol. 1, January 1983

[30] NIELSEN, D.S. *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*, Danish Atomic Energy Commission, RISO-M-1374, May 1971

[31] Nuclear Regulatory Commission, Reactor Safety Study: *An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, Rep. WASH-1400-MR (NUREG-75/014), Washington, DC, 1975

[32] PAPAZOGLOU, I. A. *Mathematical foundations of event trees, Reliability Engineering and System Safety 61* (2008) 169-183, Northern Island, 2008

[33] *Railtrack, Engineering Safety Management System*, Issue 2.0, "Yellow Book", 1997

[34] RAUSAND, M., HOYLAND, A. *System Reliability Theory – Models, Statistical Methods and Applications*, Hoboken, New Jersey, 2004

---

3 A l'étude, voir 56/1322/CD.

[35] SIU, N., Risk *Assessment for Dynamic Systems:* An Overview, Reliability Engineering and System Safety 43, 1994, p. 43-73

[36] SMITH, D.J. *Reliability, Maintainability and Risk*, Oxford, 2001

[37] Special subject: *Common cause failure analysis*, Kerntechnik Vol 71, No 1-2, Carl Hanser-Verlag, February 2006, pp 8 – 62

[38] VILLEMEUR, A. *Reliability, Availability, Maintainability and Safety Assessment*. Volume 1. Methods and Techniques, Chichester, Wiley, 1992

[39] XU, H.; DUGAN, J.B. *Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment*, University of Virginia, January 2004

[40] ZIO, E. *An Introduction to the Basics of Reliability and Risk Analysis*, Series in Quality, Reliability and Engineering Statistics, Vol. 13, 2007

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch