BS EN 62502:2011

BSI Standards Publication

Analysis techniques for dependability — Event tree analysis (ETA)

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 62502:2011. It is identical to IEC 62502:2010.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and value management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 59962 0

ICS 21.020; 29.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2011.

Amendments issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62502

November 2010

ICS 21.020

English version

Analysis techniques for dependability - Event tree analysis (ETA)
(IEC 62502:2010)

Techniques d'analyse de la sûreté de fonctionnement - Analyse par arbre d'événement (AAE) (CEI 62502:2010)

Verfahren zur Analyse der Zuverlässigkeit - Ereignisbaumanalyse (ETA) (IEC 62502:2010)

This European Standard was approved by CENELEC on 2010-11-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 62502:2010 E

Foreword

The text of document 56/1380/FDIS, future edition 1 of IEC 62502, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62502 on 2010-11-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2011-08-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-11-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 62502:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

[12] ISO/IEC 31010	NOTE	Harmonized as EN 31010.
[13] IEC 60300-3-1:2003	NOTE	Harmonized as EN 60300-3-1:2004 (not modified).
[15] IEC 60812:2006	NOTE	Harmonized as EN 60812:2006 (not modified)
[16] IEC 61078:2006	NOTE	Harmonized as EN 61078:2006 (not modified)
[17] IEC 61165:2006	NOTE	Harmonized as EN 61165:2006 (not modified)
[18] IEC 61508 series	NOTE	Harmonized in EN 61508 series (not modified)
[19] IEC 61511-3:2003	NOTE	Harmonized as EN 61511-3:2004 (not modified)
[20] IEC 61703:2001	NOTE	Harmonized as EN 61703:2002 (not modified)
[22] IEC 62429:2007	NOTE	Harmonized as EN 62429:2008 (not modified)
[23] IEC 62508:2010	NOTE	Harmonized as EN 62508:2010 (not modified)
[24] IEC 62551[1)]	NOTE	Harmonized as EN 62551[2)] (not modified)

[1)] To be published.

[2)] At draft stage.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 60050-191	1990	International Electrotechnical Vocabulary (IEV) - Chapter 191: Dependability and quality of service	-	-
IEC 61025	2006	Fault Tree Analysis (FTA)	EN 61025	2007

CONTENTS

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.

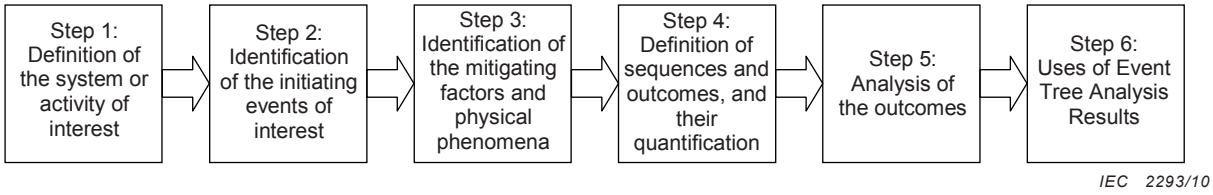

Figure 1 – Process for development of event trees

Clause 9briefly 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 8.3and 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.

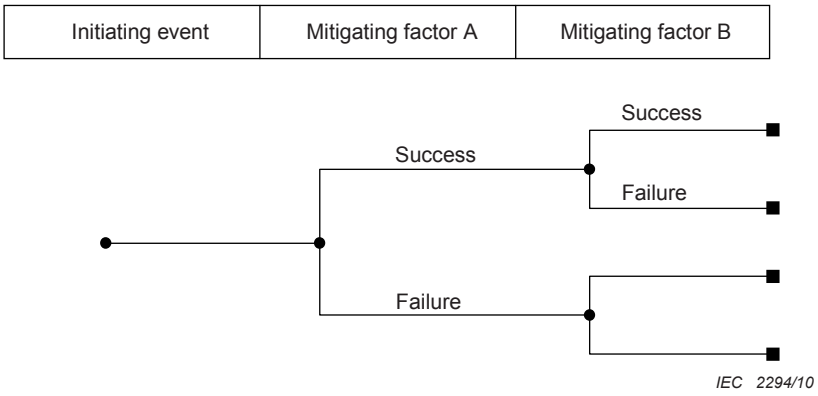

Figure 2 – Simple graphical representation of an event tree

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.

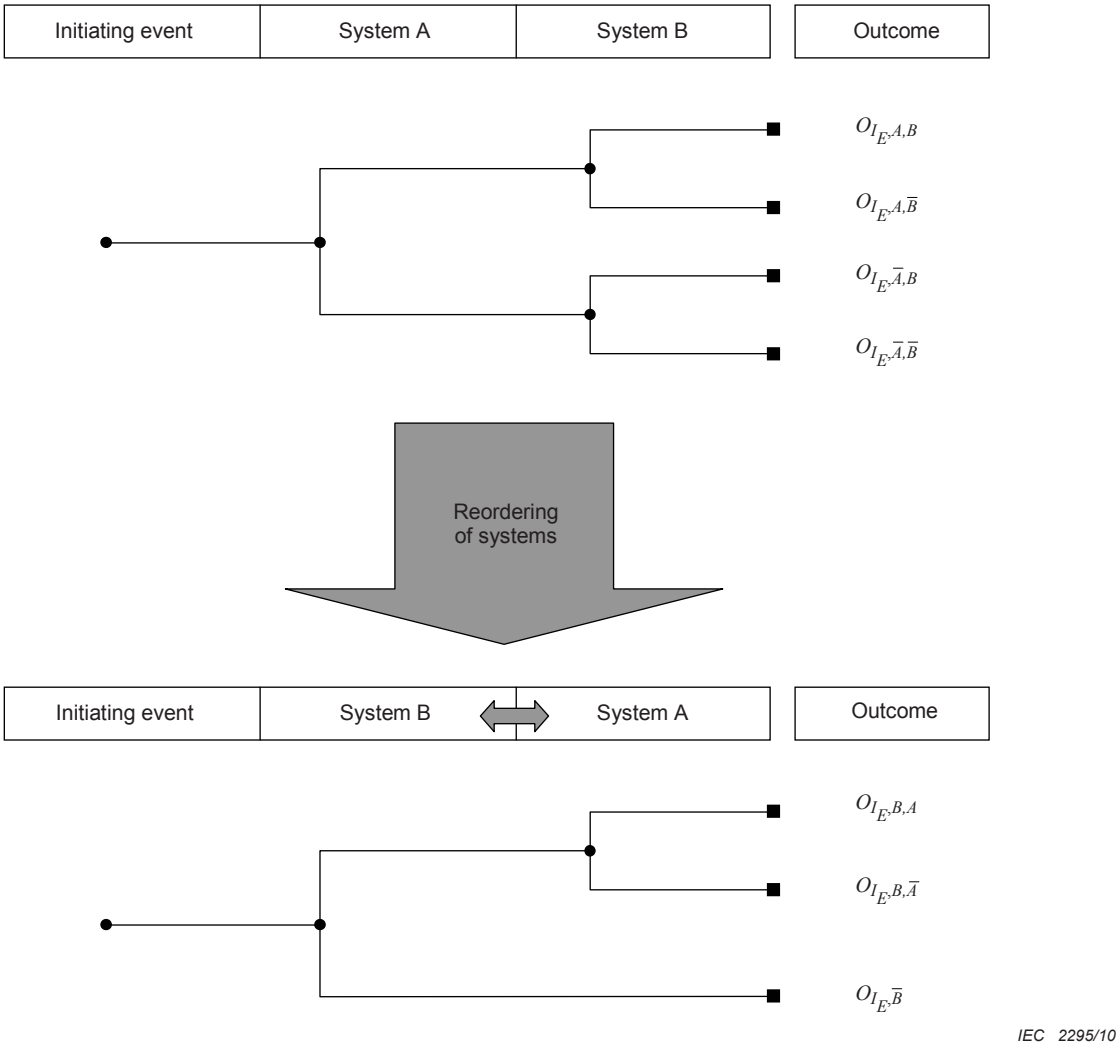

Figure 3 – Functional dependencies in event trees

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 (8.3.2and 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.

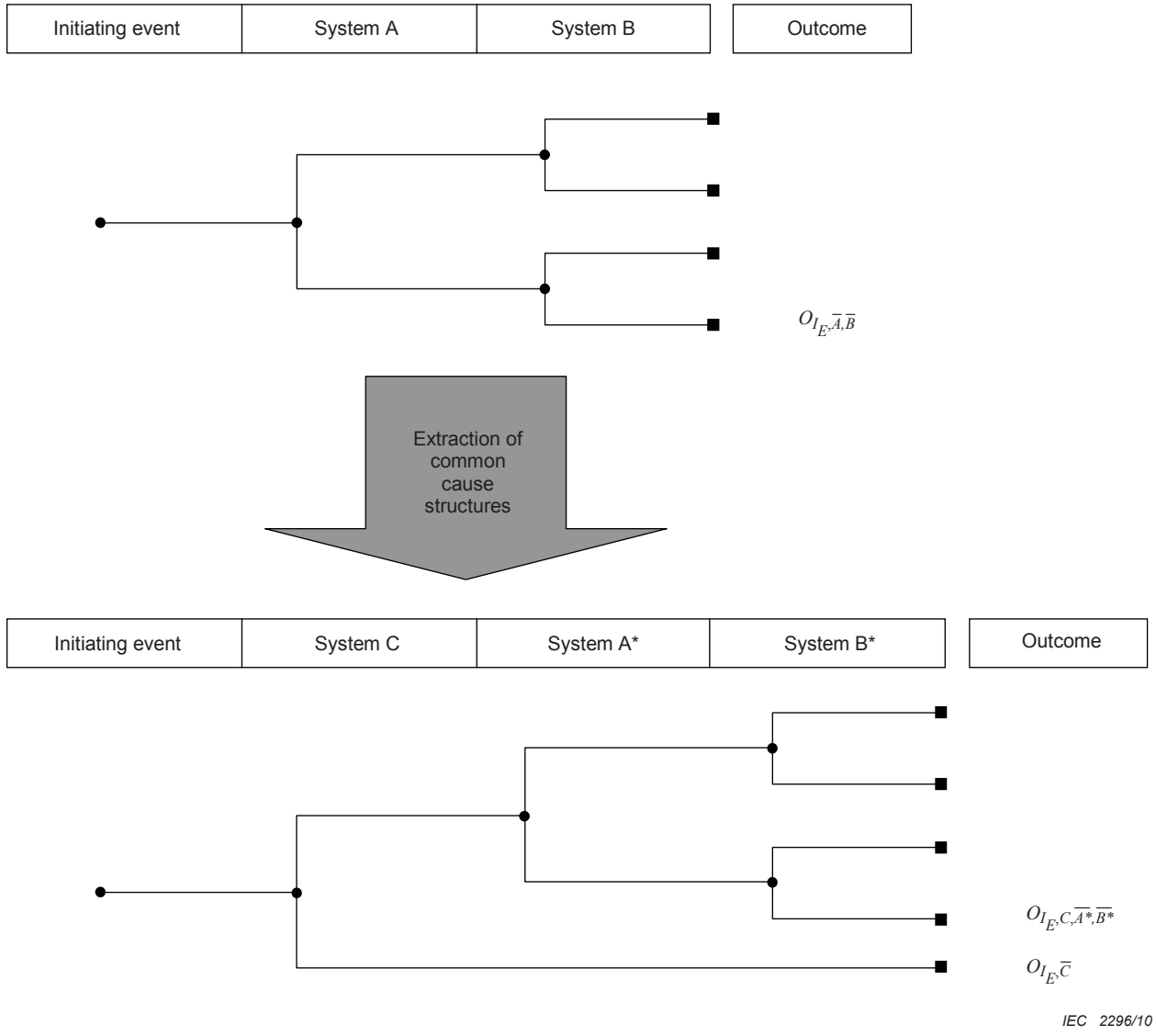

Figure 4 – Modelling of structural or physical dependencies

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.

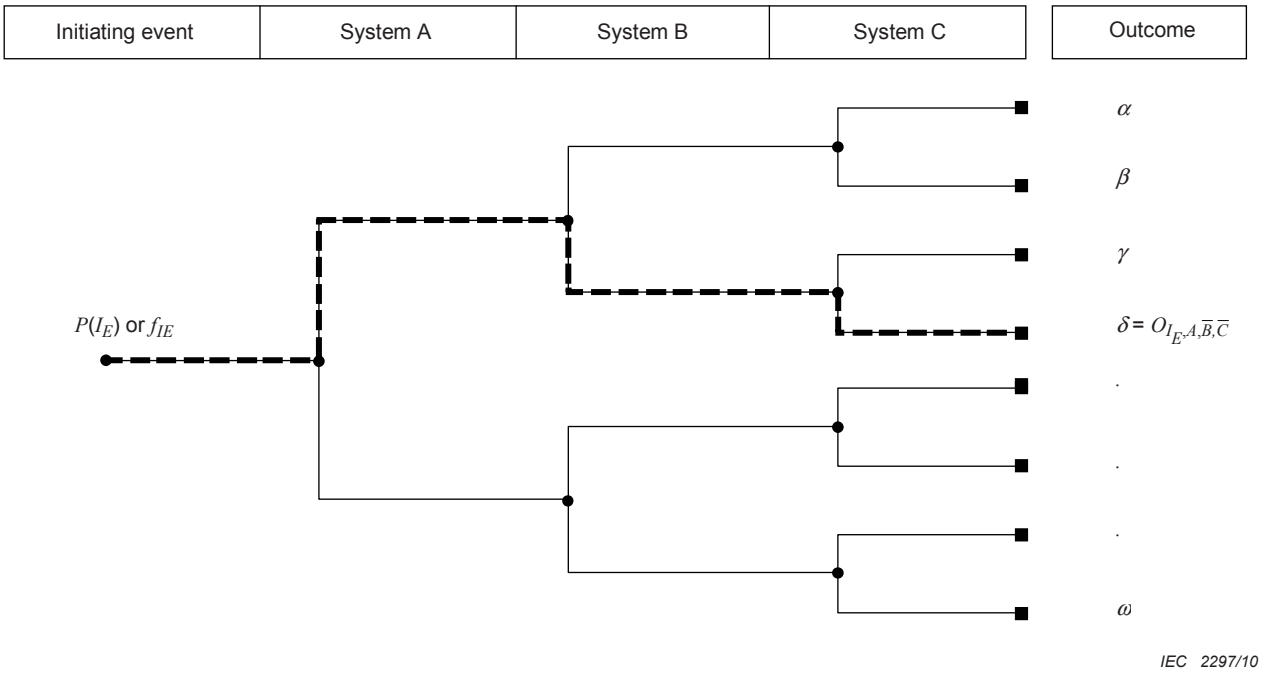

Figure 5 – Sequence of events

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 $\alpha, \beta, \gamma, \delta, \ldots, \omega$ 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].

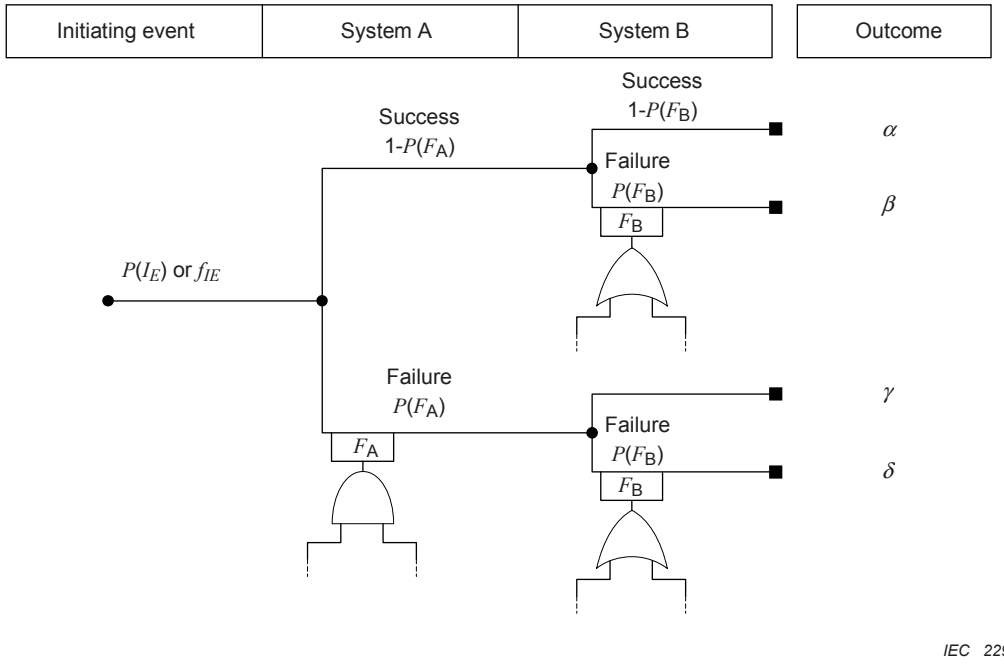

Figure 6 – Fault tree linking

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:

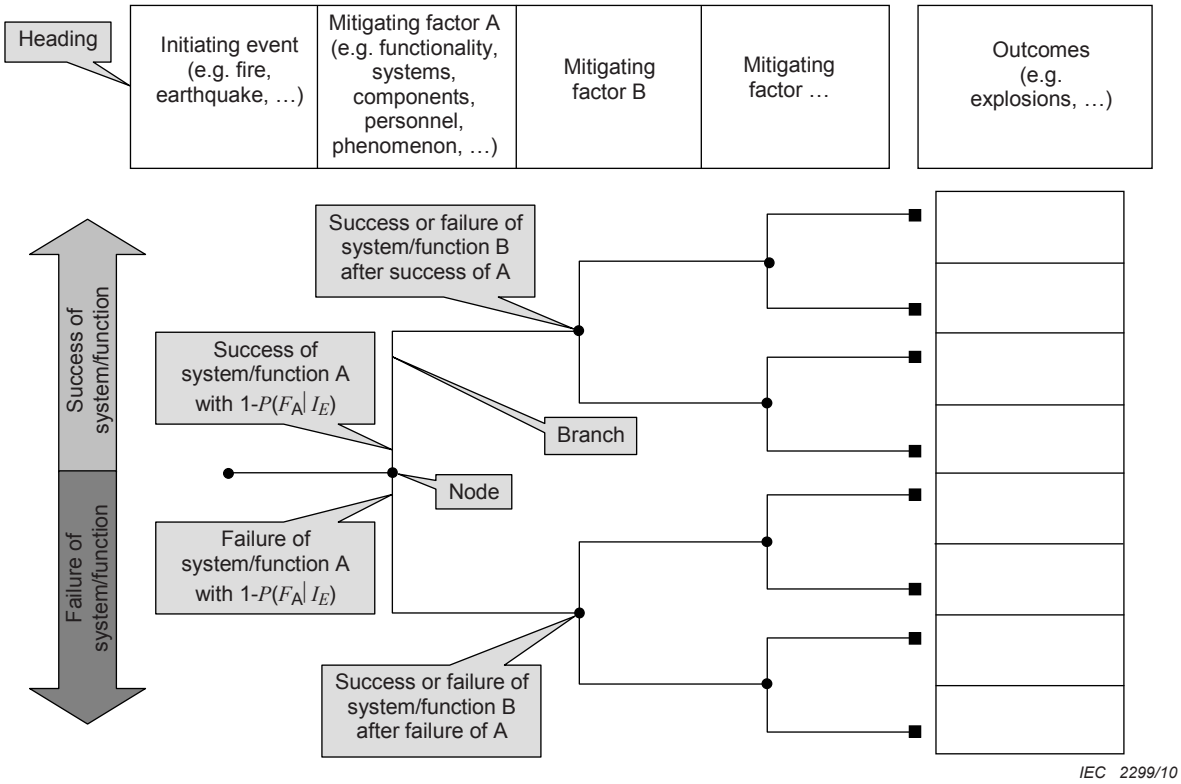

Figure A.1 – Frequently used graphical representation for event trees

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 7.2.5c)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.

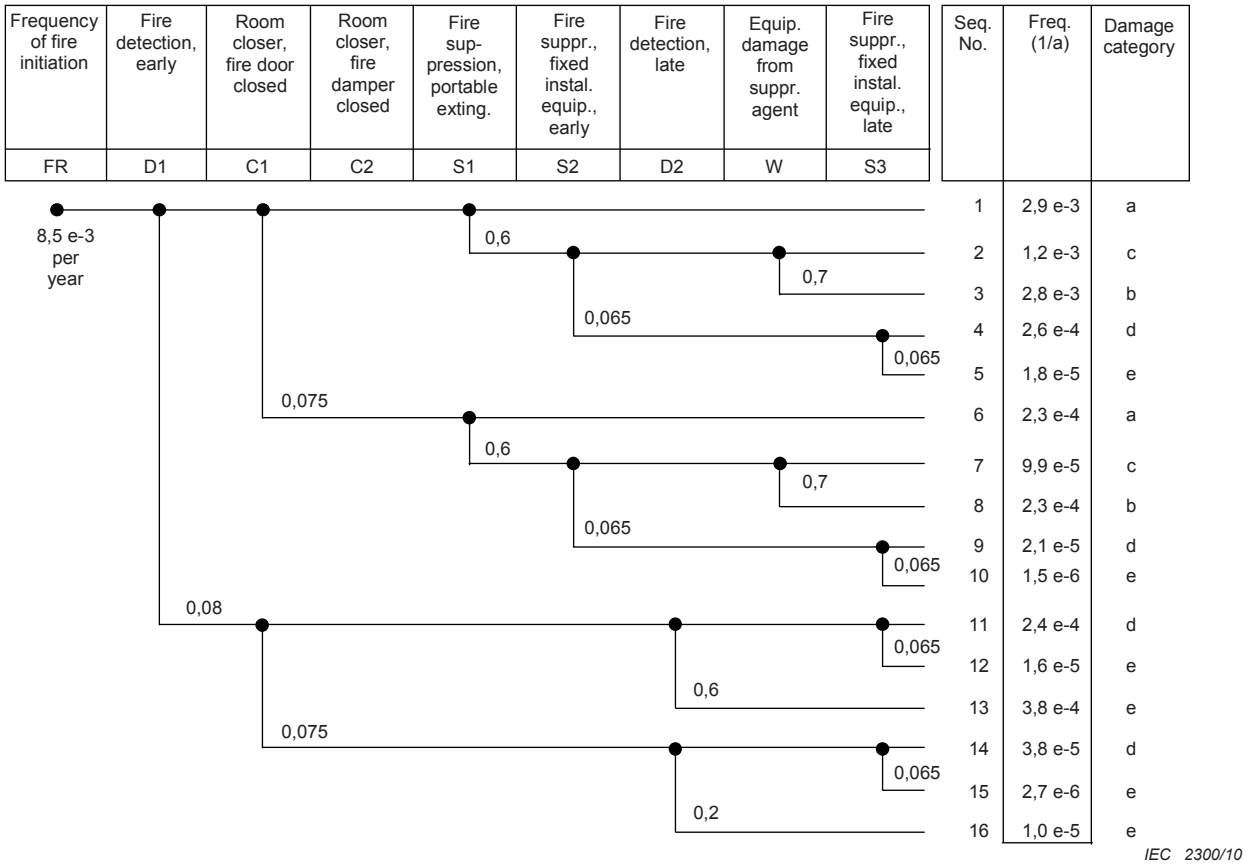

Figure B.1 – Event tree for a typical fire incident in a diesel generator building

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.

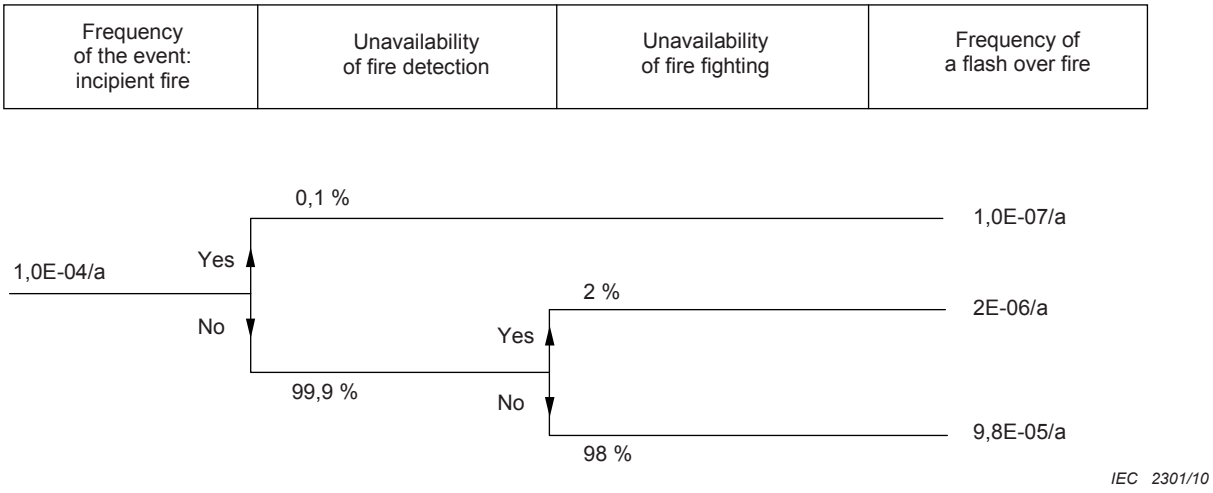

Figure B.2 – Simplified event tree for a fire event

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.

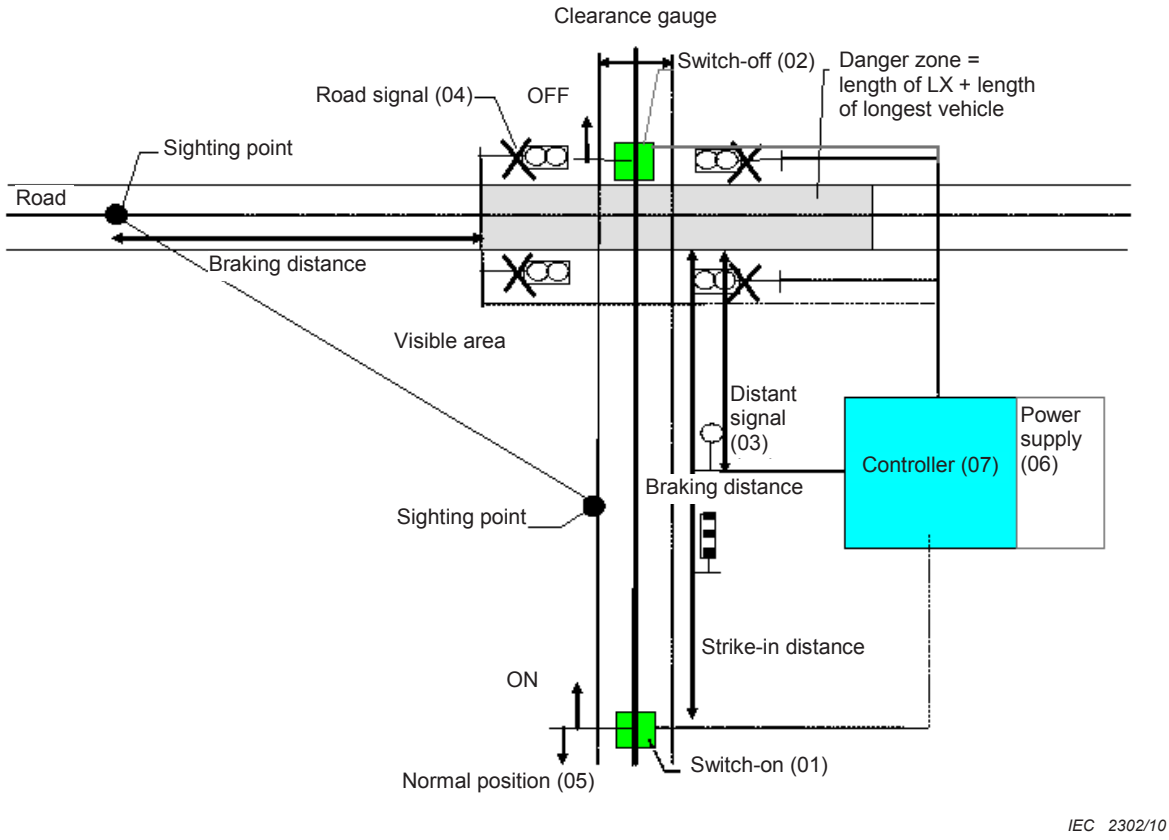

Figure B.3 – Level-crossing system (LX)

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.

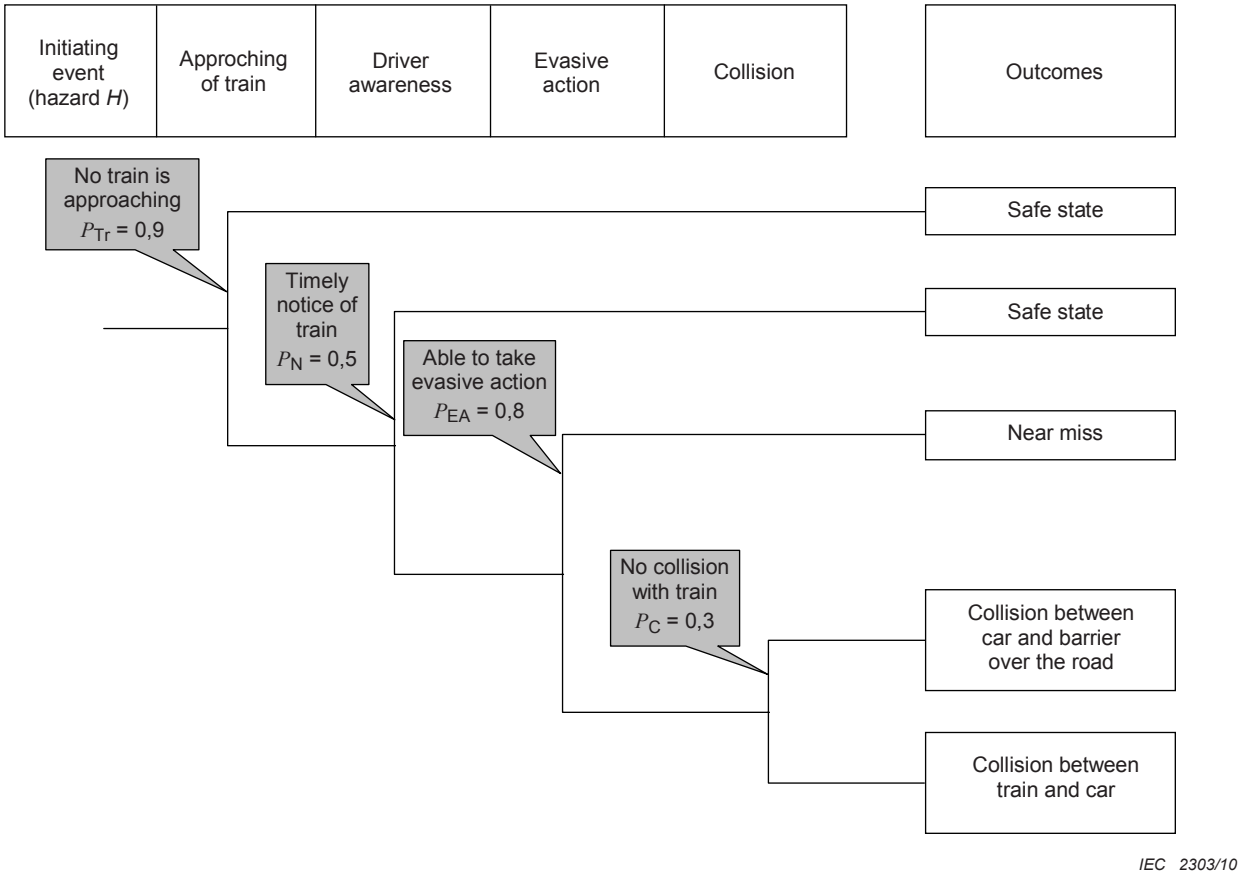

Figure B.4 – ETA for a level-crossing system

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.

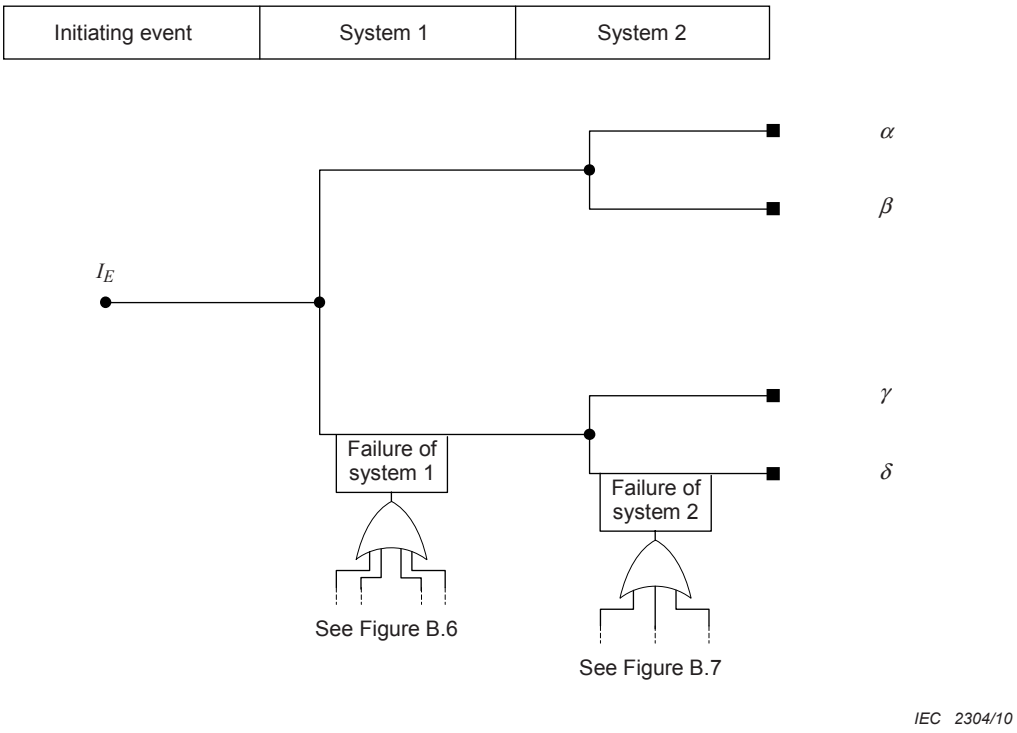

Figure B.5 – Simple example

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].

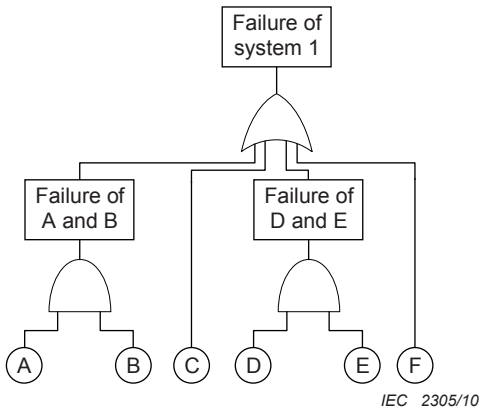

Figure B.6 – Fault tree for the failure of system 1

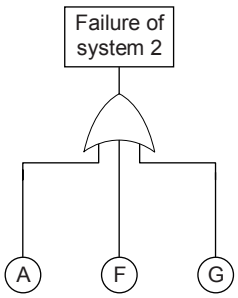

Figure B.7 – Fault tree for the failure of system 2

Together with these fault trees and the event tree, the reduced Boolean expressions for the outcomes $\alpha, \beta, \gamma, \delta$ 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.

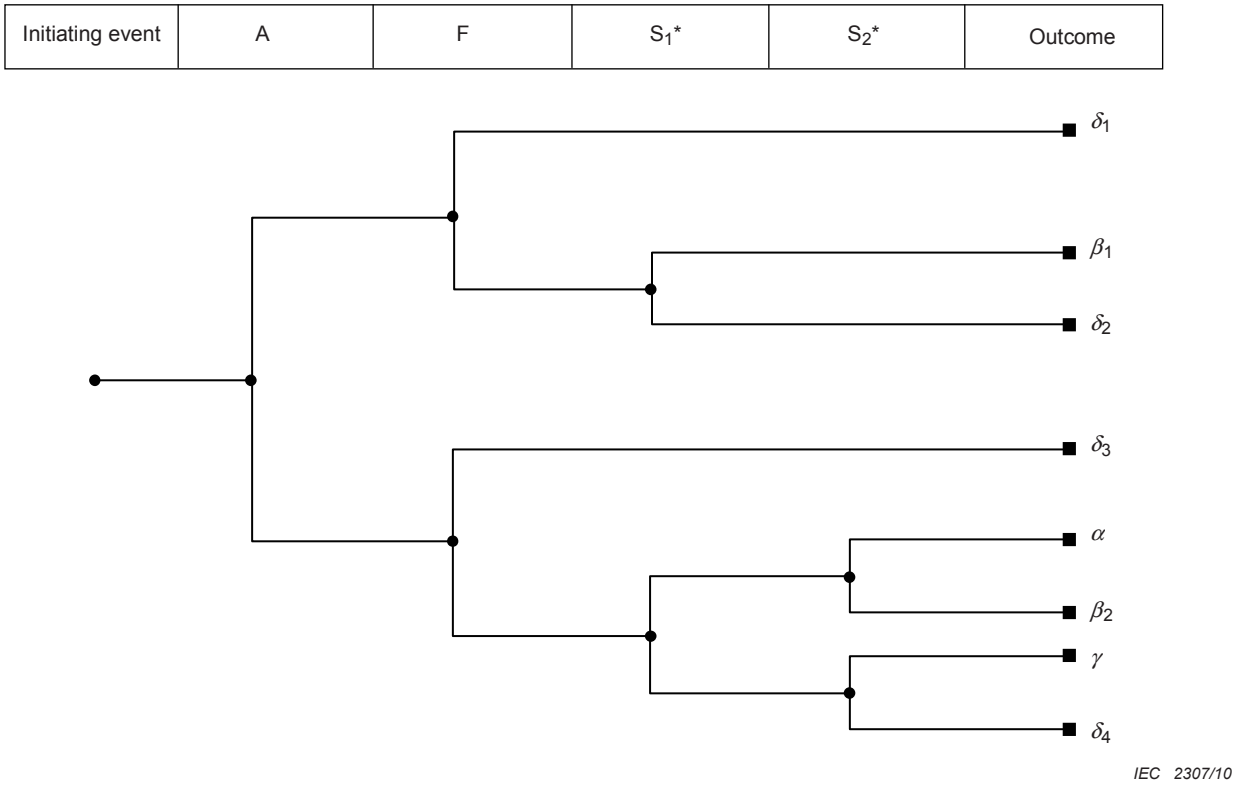

Figure B.8 – Modified event tree

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:

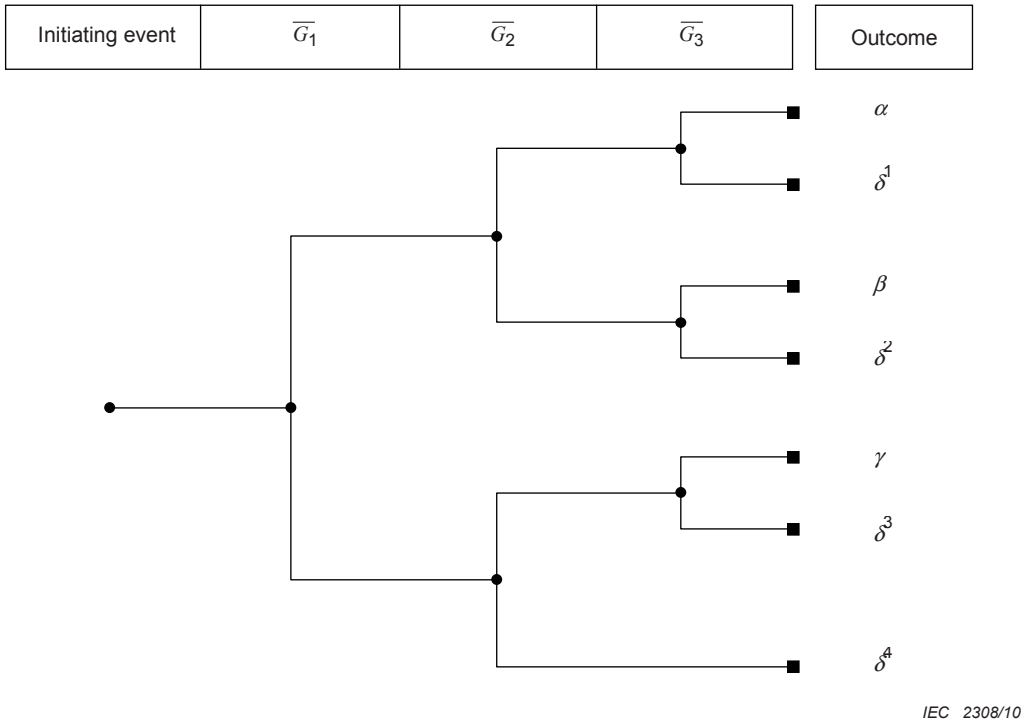

Figure B.9 – Event tree with "grouped faults"

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

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™