IEC 60300-3-1

Edition 2.0 2003-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 60300-3-1

Edition 2.0 2003-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XA
CODE PRIX

ICS 03.120.30; 21.020

ISBN 978-2-83220-664-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-1 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition, published in 1991, and constitutes a full technical revision. In particular, the guidance on the selection of analysis techniques and the number of analysis techniques covered has been extended.

This bilingual version (2013-03) corresponds to the monolingual English version, published in 2003-01.

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

FDIS	Report on voting
56/825/FDIS	56/840/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.

The French version of this standard has not been voted upon.

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 2007. 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

The analysis techniques described in this part of IEC 60300 are used for the prediction, review and improvement of reliability, availability and maintainability of an item.

These analyses are conducted during the concept and definition phase, the design and development phase and the operation and maintenance phase, at various system levels and degrees of detail, in order to evaluate, determine and improve the dependability measures of an item. They can also be used to compare the results of the analysis with specified requirements.

In addition, they are used in logistics and maintenance planning to estimate frequency of maintenance and part replacement. These estimates often determine major life cycle cost elements and should be carefully applied in life cycle cost and comparative studies.

In order to deliver meaningful results, the analysis should consider all possible contributions to the dependability of a system: hardware, software, as well as human factors and organizational aspects.

DEPENDABILITY MANAGEMENT –

Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology

1 Scope

This part of IEC 60300 gives a general overview of commonly used dependability analysis techniques. It describes the usual methodologies, their advantages and disadvantages, data input and other conditions for using various techniques.

This standard is an introduction to selected methodologies and is intended to provide the necessary information for choosing the most appropriate analysis methods.

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 (IEV) – Chapter 191: Dependability and quality of service*

IEC 60300-3-2:1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field*

IEC 60300-3-4:1996, *Dependability management – Part 3: Application guide – Section 4: Guide to the specification of dependability requirements*

IEC 60300-3-5:2001, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10:2001, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60706-1:1982, *Guide on maintainability of equipment – Part 1: Sections One, Two and Three – Introduction, requirements and maintainability programme*

IEC 60706-2:1990, *Guide on maintainability of equipment – Part 2: Section Five – Maintainability studies during the design phase*

IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61078:1991, *Analysis techniques for dependability – Reliability block diagram method*

IEC 61165:1995, *Application of Markov techniques*

IEC 61709:1996, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 61882:2001, *Hazard and operability studies (HAZOP studies) – Application guide*

ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*

3 Definitions

For the purposes of this part of IEC 60300, the definitions given in IEC 60050(191), some of which are reproduced below, together with the following definitions, apply.

3.1
item, entity
any part, component, device, sub-system, functional unit, equipment or system that can be individually considered

NOTE An item may consist of hardware, software or both, and may also in particular cases, include people.

[IEV 191-01-01]

3.2
system
set of interrelated or interacting elements

[ISO 9000, 2000]

NOTE 1 In the context of dependability, a system will have

a) a defined purpose expressed in terms of required functions, and

b) stated conditions of operation/use.

NOTE 2 The concept of a system is hierarchical.

3.3
component
item on the lowest level considered in the analysis

3.4
allocation
procedure applied during the design of an item intended to apportion the requirements for performance measures for an item to its sub-items according to given criteria

3.5
failure
termination of the ability of an item to perform a required function

NOTE 1 After failure the item has a fault.

NOTE 2 'Failure' is an event, as distinguished from 'fault', which is a state.

[IEV 191-04-01]

3.6
fault
state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

NOTE A fault is often the result of a failure of the item itself, but may exist without prior failure.

[IEV 191-05-01]

4 Basic dependability analysis procedure

4.1 General procedure

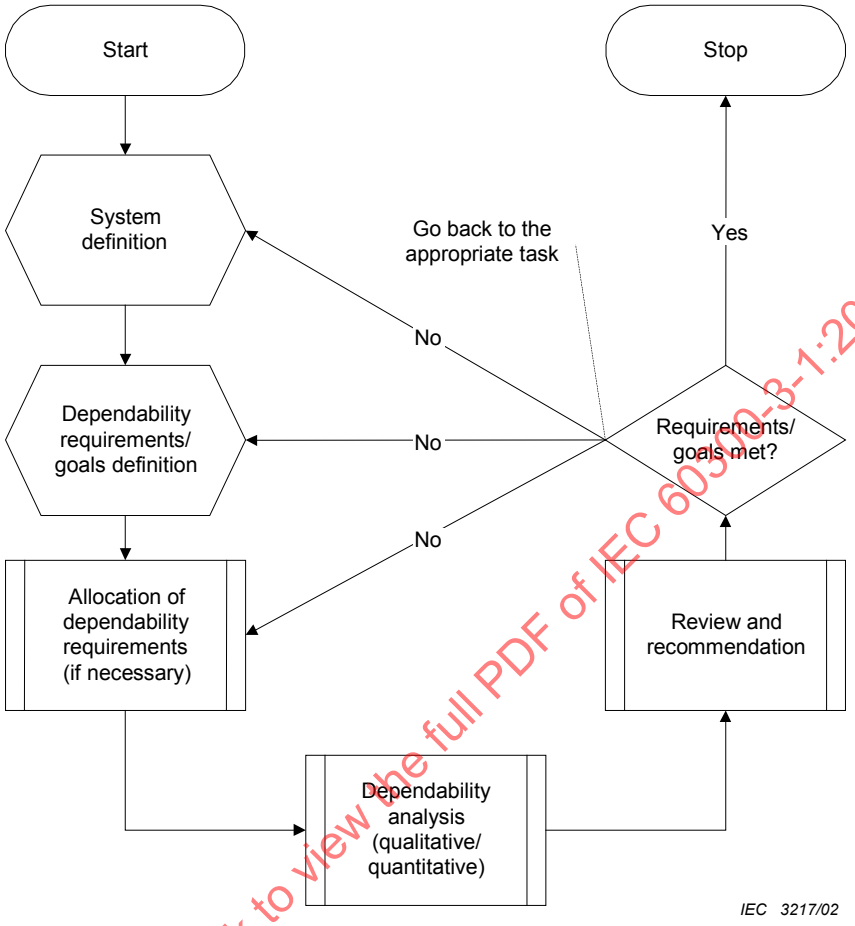


Figure 1 – General dependability analysis procedure

A general dependability analysis procedure consists of the following tasks (as applicable):

a) System definition

Define the system to be analysed, its modes of operation, the functional relationships to its environment including interfaces or processes. Generally the system definition is an input from the system engineering process.

b) Dependability requirements/goals definition

List all system reliability and availability requirements or goals, characteristics and features, together with environmental and operating conditions, as well as maintenance requirements. Define system failure, failure criteria and conditions based on system functional specification, expected duration of operation and operating environment (mission profile and mission time). IEC 60300-3-4 should be used as guidance.

c) Allocation of dependability requirements

Allocate system dependability requirements or goals to the various sub-systems in the early design phase when necessary.

d) Dependability analysis

Analyse the system usually on the basis of the dependability techniques and relevant performance data.

1) Qualitative analysis
   - Analyse the functional system structure.
   - Determine system and component fault modes, failure mechanisms, causes, effects and consequences of failures.
   - Determine degradation mechanism that may cause failures.
   - Analyse failure/fault paths.
   - Analyse maintainability with respect to time, problem isolation method, and repair method.
   - Determine the adequacy of the diagnostics provided to detect faults.
   - Analyse possibility for fault avoidance.
   - Determine possible maintenance and repair strategies, etc.
2) Quantitative analysis
   - Develop reliability and/or availability models.
   - Define numerical reference data to be used.
   - Perform numerical dependability evaluations.
   - Perform component criticality and sensitivity analyses as required.

e) Review and recommendations

Analyse whether the dependability requirements/goals are met and if alternative designs may cost effectively enhance dependability. Activities may include the following tasks (as appropriate):

- Evaluate improvement of system dependability as a result of design and manufacture improvement (e.g. redundancy, stress reduction, improvement of maintenance strategies, test systems, technological processes and quality control system).

  NOTE 1 The inherent dependability performance measures can be improved only by design. When poor measured values are observed due to bad manufacturing processing, from the operating point of view, observed dependability performance measures can be enhanced by improving the manufacturing process.

- Review system design, determine weaknesses and critical fault modes and components.
- Consider system interface problems, fail-safe features and mechanisms, etc.
- Develop alternative ways for improving dependability, e.g. redundancy, performance monitoring, fault detection, system reconfiguration techniques, maintenance procedures, component replaceability, repair procedures.
- Perform trade-off studies evaluating the cost and complexity of alternative designs.
- Evaluate the effect of manufacturing process capability.
- Evaluate the results and compare with requirements.

NOTE 2 The general procedure summarizes, from an engineering point of view, the specific dependability programme elements from IEC 60300-2, which are applicable for dependability analysis: dependability specifications, analysis of use environment, reliability engineering, maintainability engineering, human factors, reliability modelling and simulation, design analysis and product evaluation, cause-effect impact and risk analysis, prediction and trade-off analysis.

4.2 Dependability analysis methods

The methods presented in this standard fall into two main categories:

- methods which are primarily used for dependability analysis;
- general engineering methods which support dependability analysis or add value to design for dependability.

The usability of the dependability analysis methods within the general dependability analysis tasks of the general analysis procedure is given in Table 1. Table 2 gives more detailed characteristics. The methods are explained briefly in Annex A.

Table 1 – Use of methods for general dependability analysis tasks

Analysis method	Allocation of dependability requirements/goals	Qualitative analysis	Quantitative analysis	Review and recommen-dations	Annex
Failure rate prediction	Applicable for serial systems without redundancy	Possible for maintenance strategy analysis	Calculation of failure rates and MTTF for electronic components and equipment	Supporting	A.1.1
Fault tree analysis	Applicable, if system behaviour is not heavily time- or sequence-dependent	Fault combinations	Calculation of system reliability, availability and relative contributions of subsystems to system unavailability	Applicable	A.1.2
Event tree analysis	Possible	Failure sequences	Calculation of system failure rates	Applicable	A.1.3
Reliability block diagram analysis	Applicable, for systems where independent blocks can be assumed	Success paths	Calculation of system reliability, availability	Applicable	A.1.4
Markov analysis	Applicable	Failure sequences	Calculation of system reliability, availability	Applicable	A.1.5
Petri net analysis	Applicable	Failure sequences	To provide the system description for Markov analysis	Applicable	A.1.6
Failure modes and effects (and criticality) analysis; FME(C)A	Applicable for systems where independent single failure is predominant	Effects of failures	Calculation of system failure rates (and criticality)	Applicable	A.1.7
HAZOP studies	Supporting	Causes and consequences of deviations	Not applicable	Supporting	A.1.8
Human reliability analysis	Supporting	Impact of human performance on system operation	Calculation of error probabilities for human tasks	Supporting	A.1.9
Stress-strength analysis	Not applicable	Usable as a means of fault avoidance	Calculation of reliability for (electro) mechanical components	Supporting	A.1.10
Truth table (structure function analysis)	Not applicable	Possible	Calculation of system reliability, availability	Supporting	A.1.11
Statistical reliability methods	Possible	Impact of faults	Quantitative estimation of reliability with uncertainties	Supporting	A.1.12

NOTE The particular wording in the table is used as follows:

'Applicable' means that the method is generally applicable and recommended for the task (possibly with the mentioned restrictions).

'Possible' means that the method may be used for this task but has certain drawbacks compared to other methods.

'Supporting' means that the method is generally applicable for a certain part of the task but not as a stand-alone method for the complete task.

'Not applicable' means that the method cannot be used for this task.

Among the supporting or general engineering methods are (the list being not necessarily exhaustive):

– maintainability studies (covered by IEC 60300-3-10 in general and IEC 60706-2 in particular);
– sneak circuit analysis (A.2.1);
– worst case analysis (A.2.2);
– variation simulation modelling (A.2.3);
– software reliability engineering (A.2.4);
– finite element analysis (A.2.5);
– parts derating and selection (A.2.6);
– Pareto analysis (A.2.7);
– cause and effect diagrams (A.2.8);
– failure reporting and corrective action system (A.2.9).

It should also be noted that the methods are named and understood in the sense of the relevant IEC standards (where they exist). The following methods have not been included as separate methods because they are derived from or closely related to primary methods:

– cause/consequence analysis is a combination of ETA and FTA;
– dynamic FTA is an extension of FTA, where certain events are expressed by Markov sub-models;
– functional failure analysis is a particular type of functional FMEA;
– binary decision diagrams are mainly used as an efficient representation of fault trees.

4.3 Dependability allocations

Defining the dependability requirements for sub-systems is an essential part of the system design work. The objective of this task is to find the most effective system architecture to achieve the dependability requirements (and thus contribute to the feasibility study). As dependability is the collective term for reliability, availability and maintainability, an allocation for each of these characteristics is necessary. However as allocation techniques for all three characteristics are similar, the collective term dependability is used in this instance.

The first step is to allocate the dependability requirements of the overall system to sub-systems, depending on the complexity of these sub-systems based on experience with comparable sub-systems. If the requirements are not met by the initial design, allocation and/or design shall be repeated. Allocation is also often made on the basis of considerations such as complexity, criticality, operational profile and environmental condition.

Since dependability allocation is normally required at an early stage when little or no information is available, the allocation should be updated periodically.

Allocation, sometimes called apportionment, of system dependability to the sub-system and assembly levels is necessary early in the product definition phase in order to

– check the feasibility of dependability requirements for the system,
– establish realistic dependability design requirements at lower levels,
– establish clear and verifiable dependability requirements for sub-suppliers.

When accomplishing dependability allocation, the following steps are needed:

– Analyse the system and identify areas where design is known and information concerning values of dependability characteristics is available or can be readily assessed.
– Assign the appropriate weights and determine their contribution to the top-level system dependability requirement. The difference constitutes the portion of the dependability requirement that can be allocated to the other areas.

Dependability allocation has the following benefits:

– It provides a way for the product development to progress and to understand the dependability goals relationships between system and their items (e.g. sub-systems, equipment, components).
– It considers dependability equally with other design parameters such as cost and performance characteristics.
– It provides specific dependability goals for the suppliers to meet for their deliveries, which, in turn, leads to improved design and procurement procedures.
– It may lead to optimum system dependability because it considers such factors as complexity, criticality and effect of operational environment.

On the other hand, some limitations should be noted:

– Assumption is often made that the items of a system are independent, i.e. failure of one item does not affect others. Since this assumption is often not valid, this limitation reduces the benefits of the method.
– Allocation of redundant systems is more complex. In these cases, it is appropriate to use an iterative method to check whether dependability goals for the system can be reached, for example the fault tree method.

4.4 Dependability analysis

4.4.1 Categories of methods

Dependability analysis methods, which are explained briefly in Annex A, can be classified by the following categories with regard to their main purpose:

a) methods for fault avoidance, e.g.
   1) parts derating and selection,
   2) stress-strength analysis;

b) methods for architectural analysis and dependability assessment (allocation), e.g.
   1) bottom-up method (mainly dealing with effects of single faults),
      – event tree analysis (ETA),
      – failure mode and effects analysis (FMEA),
      – hazard and operability study (HAZOP);
   2) top-down methods (able to account for effects arising from combination of faults)
      – fault tree analysis (FTA),
      – Markov analysis,
      – Petri net analysis,
      – truth table (structure function analysis),
      – reliability block diagrams (RBD);

c) methods for estimation of measures for basic events, e.g.
   - failure rate prediction,
   - human reliability analysis (HRA),
   - statistical reliability methods,
   - software reliability engineering (SRE).

Another distinction is whether these methods work with sequences of events or time-dependent properties. If this is taken into account, the following comprehensive categorization results:

Sequence dependent	Event-tree analysis	Markov, Petri, truth table
Sequence independent	FMEA, HAZOP	FTA, RBD
	Bottom-up (single fault)	**Top-down (multiple faults)**

These analysis methods allow for the evaluation of qualitative characteristics as well as estimation of quantitative ones in order to predict long-term operating behaviour. It should be noticed that the validity of any result is clearly dependent on the accuracy and correctness of the input data for the basic events.

However, no single dependability analysis method is sufficiently comprehensive and flexible to deal with all the possible model complexities required to evaluate the features of practical systems (hardware and software, complex functional structures, various technologies, repairable and maintainable structures, etc.). It may be necessary to consider several complementary analysis methods to ensure proper treatment of complex or multi-functional systems.

In practice, a composite approach, with top-down and bottom-up analysis complementing one another, has proven to be very effective, in particular with respect to ensuring the completeness of the analysis.

4.4.2 Bottom-up methods

The starting point of any bottom-up method is to identify failure modes at the component level. For each failure mode, the corresponding effect on performance is deduced for the appropriate system level. This “bottom-up” method is rigorous in identifying all single-failure modes, because it can rely on parts lists or other checklists. In the initial stages of development, the analysis may be qualitative in nature and deal with functional failures. Later, as the component design details become available a quantitative analysis can be undertaken.

4.4.3 Top-down methods

At first, the undesirable single event or system success at the highest level of interest (the top event) should be defined. The contributory causes of that event at all levels are then identified and analysed.

The starting point of the top-down approach is to proceed from the highest level of interest, that is, the system or sub-system level, to successively lower levels in order to identify undesirable system operations.

The analysis is performed at the next lowest system level to identify any failure and its associated failure mode, which could result in the failure effect as originally identified. For each of these second level failures, the analysis is repeated by tracing back along the functional paths and relationships to the next lowest level. This process is continued as far as the lowest level desired.

The top-down approach is used for evaluating multiple failures including sequentially related failures, the existence of faults due to a common cause, or wherever system complexity makes it more convenient to begin by listing system failures.

4.5 Maintenance and repair analysis and considerations

The performance of a repairable system is greatly influenced by the system maintainability as well as the repair or maintenance strategies employed. The availability performance measure is the appropriate measure for evaluating the influence of maintenance and repair on system dependability when long-term provision of function is the critical requirement. Reliability is the appropriate performance measure when continuous provision of function is the critical requirement.

Repair of a system during operation without interruption of its function is normally possible only for a redundant system structure with accessible redundant components. If so, then repair or replacement increases system reliability performance and availability performance.

It is usually necessary to perform a separate analysis to evaluate repair and maintenance aspects of a system (see IEC 60706-1, IEC 60706-2 and IEC 60300-3-10).

5 Selecting the appropriate analysis method

Selecting methods to implement into a dependability programme is a highly individualized process, so much so that a general suggestion for a selection of one or more of the specific methods cannot be made. The selection of appropriate methods should be carried out by a joint effort of experts from the dependability and system engineering field. Selection should be made early in the programme development and should be reviewed for applicability.

Selecting methods can be made easier, however, by using the following criteria:

a) System complexity: complex systems, e.g. involving redundancy or diversity features, usually demand a deeper level of analysis than simpler systems.

b) System novelty: a completely new system design may require a more thorough level of analysis than a well-proven design.

c) Qualitative versus quantitative analysis: is a quantitative analysis necessary?

d) Single versus multiple faults: are effects arising from combination of faults relevant or can they be neglected?

e) Time or sequence-dependent behaviour: does the sequence of events play a role in the analysis (e.g. the system fails only if event A is preceded by B, not vice versa) or does the system exhibit time-dependent behaviour (e.g. degraded modes of operation after failure, phased missions)?

f) Can be used for dependent events: are the failure or repair characteristics of an individual item dependent on the state of the system?

g) Bottom-up versus top-down analysis: usually bottom-up methods can be applied in a more straightforward manner, while top-down methods need more thought and creativity and may therefore be more error-prone.

h) Allocation of reliability requirements: should the method be capable of quantitative allocation of reliability requirements?

i) Mastery required: what level of education or experience is required in order to meaningfully and correctly apply the method?

j) Acceptance and commonality: is the method commonly accepted, e.g. by a regulatory authority or a customer?

k) Need for tools support: does the method need (computer) tool support or can it also be performed manually?

l) Plausibility checks: is it easy to inspect the plausibility of the results manually? If not, are the tools available validated?

m) Availability of tools: are tools available either in-house or commercially? Do these tools have a common interface with other analysis tools so that results may be re-used or exported?

n) Standardization: is there a standard which describes the feature of the method and the presentation of results (e.g. symbols)?

Table 2 gives an overview of various dependability analysis methods and their characteristics and features. More than one method may be required to provide a complete analysis of a system.

Table 2 – Characteristics of selected dependability analysis methods

Method	Suitable for complex systems	Suitable for novel system designs	Quantitative analysis	Suitable for combination of faults	Suitable to handle sequence-dependence	Can be used for dependent events	Bottom-up or top-down	Suitable for depend-ability allocation	Mastery required (from low to high)	Acceptance and commonality	Need for tool support	Plausibility checks	Availability of tools	IEC standard
Failure rate prediction	No	Yes	Yes	No	No	No	BU	Yes	Low	High	Avg	Yes	High	61709
Fault tree analysis (FTA)	Yes	Yes	Yes	Yes	No	No	TD	Yes	Avg	High	Avg	Yes	High	61025
Event tree analysis (ETA)	NR	NR	Yes	NR	Yes	Yes	BU	NR	High	Avg	Avg	Yes	Avg	
Reliability block diagram analysis (RBD)	NR	NR	Yes	Yes	No	No	TD	Yes	Low	Avg	Avg	Yes	Avg	61078
Markov analysis	Yes	Yes	Yes	Yes	Yes	Yes	TD	Yes	High	Avg	High	No	Avg	61165
Petri net analysis	Yes	Yes	Yes	Yes	Yes	Yes	TD	Yes	High	Low	High	No	Low	
Failure mode and effects analysis (FMEA)	NR	NR	Yes	No	No	No	BU	NR	Low	High	Low	Yes	High	60812
HAZOP studies	Yes	Yes	No	No	No	No	BU	No	Low	Avg	Low	Yes	Avg	61882
Human reliability analysis	Yes	Yes	Yes	Yes	Yes	Yes	BU	No	High	High	Avg	Yes	Avg	
Stress-strength analysis	NA	NA	Yes	NA	NA	No	NA	No	High	Avg	High	Yes	Avg	
Truth table	No	Yes	Yes	Yes	No	No	NA	Yes	High	Avg	High	No	Low	
Statistical reliability methods	Yes	Yes	Yes	Yes	Yes	Yes	NA	NR	High	Avg	High	Avg	Low	60300-3-5

NR May be used for simple systems, Not recommended as a stand-alone method, to be used jointly with other methods.

TD Top-down.

BU Bottom-up.

Avg Average.

NA The criterion is not applicable with respect to this method.

Annex A
(informative)

Brief description of analysis techniques

A.1 Primary dependability analysis techniques

A.1.1 Failure rate prediction

A.1.1.1 Description and purpose

Failure rate prediction is a method that is applicable mostly during the conceptual and early design phases, to estimate equipment and system failure rate. It can also be used in the manufacturing phase for product improvement.

Three basic techniques can be adopted:

– failure rate prediction at reference conditions, also called parts count analysis;
– failure rate prediction at operating conditions, also called parts stress analysis;
– failure rate prediction using similarity analysis.

The choice of which technique to use depends on the available level of knowledge of the system at the moment the reliability prediction is performed and also on the acceptable degree of approximation.

A.1.1.2 Failure rate prediction at reference conditions and failure rate prediction at operating conditions

In the first two cases, the analyst needs to know the number and type of components that constitute the system. The analyst also needs to know the operating conditions for which the failure rate prediction is being performed. If the operating conditions are the same as the reference conditions for the components, then no account of the operating conditions needs to be made. However, when the failure rate prediction is for operating conditions that differ from the reference conditions, then the specific application conditions of the component are taken into account (electric, thermal, environmental) using models developed for the purpose. For accurate predictions, a reliable failure rate database is needed. IEC 61709 gives recommendations on how failure rates can be stated at so-called “reference conditions” in such a database, but it does not contain failure rate data. Several failure rate data handbooks have been developed and some of them are commercially available. However, reliability calculations can be time-consuming and therefore commercial software tools are available to perform these calculations.

Failure rate prediction is based upon the following assumptions:

– components are logically connected in series (i.e. each one is necessary for the system);
– component failure rates are constant over time;
– component failures are independent.

These assumptions need to be discussed with reference to the system under study since they can lead to a worst-case estimate when redundancies at the higher levels of assembly are present.

Assuming that the failure rates are constant greatly reduces the computation effort, since the total failure rate is simply the sum of the parts failure rates. This does not necessarily imply that the total failure rate is a meaningful reliability characteristic: not all failures will affect the systems in the same way. Failures of diagnostic elements as well as some fault modes may not affect system functionality. In this case, the total failure rate only provides a measure of the number of corrective maintenance actions, regardless as to whether they are related or not to system functional failures.

A reliability prediction of a system will yield predictions at an acceptable precision level, depending on the component failure models available. The same applies when the failure rate prediction in operating conditions is performed.

A.1.1.3 Failure rate prediction using similarity analysis

Similarity analysis includes the use of fielded (in-service) equipment performance data to compare new designed equipment with predecessor equipment for predicting end item reliability.

Comparisons of similar equipment may be made at the end item, sub-assembly, or component levels using the same field data, but applying different algorithms and calculation factors to the various elements. Elements to be compared may include:

– operating and environmental conditions (measured and specified);
– design features;
– design processes;
– reliability assurance processes;
– manufacturing processes;
– maintenance processes;
– components and materials.

For each of the above elements, a number of sub-elements should be compared. As examples, operating and environmental conditions may include steady-state temperature, humidity, temperature variations, electrical power, duty cycle, mechanical vibration, etc.; equipment design features may include number of components (separated according to major component family), number of circuit card assemblies, size, weight, materials, etc.

Similarity analysis should include necessary algorithms or calculation methods used to quantify similarities and differences between the equipment being assessed and the predecessor equipment.

Element similarity analysis is used when a similarity analysis is not possible because no predecessor equipment is sufficiently similar or available for a one-to-one comparison with the newly designed equipment being assessed. Element similarity analysis is the structured comparison of elements of the new equipment with similar elements of a number of different predecessor equipment, for which reliability data are available.

A.1.1.4 Benefits

– Time and cost of analysis are very low, provided reference data and models are available.
– The necessary input information and data are small and therefore adapted to the situation in the early design and development phase.
– Basic information on component reliability is gained in the early design and development phase.
– Adapted to manual and computerized calculations.
– Little training is necessary.

A.1.1.5 Limitations

– The functional structure (e.g. lower level redundancies) of a system cannot be considered, and therefore only simple structures lend themselves to parts count analysis.

– The precision level of the predictions may be low, especially for small sub-systems and limited run productions, since published or collected data are valid only statistically, i.e. they require large samples.

– The evaluation of failure modes and mechanisms and their effects is not possible.

A.1.1.6 Standards

The applicable IEC standard is IEC 61709.

A.1.1.7 **Example for an integrated circuit** (as given in IEC 61709)

For a bipolar random access memory, the failure rate is stated as $\lambda_{\text{ref}} = 10^{-7}\ h^{-1}$ in a trustworthy database based on the following reference conditions stated in IEC 61709:

– reference ambient temperature: $\theta_{\text{amb, ref}}$ of 40 °C;

– reference self-heating: 20 °C.

What is the value of the failure rate at an ambient temperature of $\theta_{\text{amb}} = 70$ °C with the same self-heating?

Step 1: The failure rate model at operating conditions is stated in IEC 61709 as $\lambda = \lambda_{\text{ref}} \times \pi_T$.

Step 2: From Figure A.1 (taken from IEC 61709), the factor for temperature influence follows to π_T = 3,4,

– using the reference virtual junction temperature
$\theta_1 = \theta_{\text{amb, ref}} + \Delta T_{\text{ref}} =$ 40 °C +20 °C = 60 °C,

– and the actual virtual junction temperature
$\theta_2 = \theta_{\text{amb}} + \Delta T_{\text{ref}} =$ 70 °C + 20 °C = 90 °C.

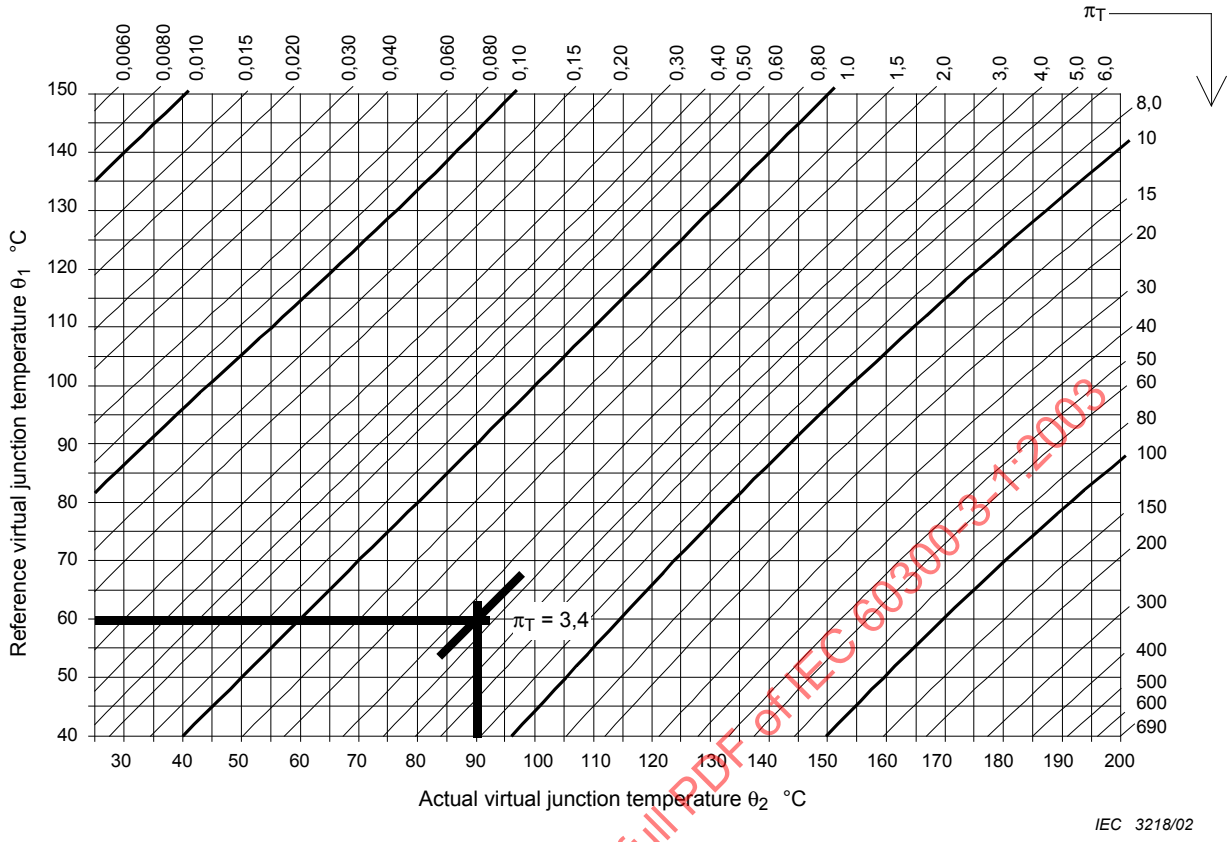


Figure A.1 – Temperature dependence of the failure rate

Step 3: The failure rate at $\theta_{amb} = 70\,°C$ is obtained as $\lambda = \lambda_{ref} \times \pi_T = 10^{-7}\,h^{-1} \times 3{,}4 = 3{,}4 \times 10^{-7}\,h^{-1}$.

A.1.2 Fault tree analysis (FTA)

A.1.2.1 Description and purpose

Fault tree analysis (FTA) is a top-down approach for analysing product dependability. It is concerned with the identification and analysis of conditions and factors which cause, or contribute to, the occurrence of a defined undesirable outcome and which affect product performance, safety, economy, or other specified characteristics.

The FTA can also be constructed to provide a system reliability prediction model and allow trade-off studies in a product design phase.

Used as a tool for detection and quantitative evaluation of a fault cause, FTA represents an efficient method that identifies and evaluates the failure modes and causes of known or suspected effects.

Taking into consideration known unfavourable effects and the ability to find respective failure modes and causes, FTA allows timely mitigation of potential failure modes allowing product dependability improvement in product design phase.

Constructed to represent hardware and software architecture as well as dealing with functionality, FTA, developed to deal with basic events, becomes a systematic reliability modelling technique that takes into account complex interactions of system parts by modelling their functional or failure dependencies, failure enabling events, common cause events, and by allowing network representation.

In order to estimate system reliability and availability using the FTA technique, methods such as Boolean reduction and cut set analysis are employed. The basic data required are component failure rates, repair rates, probability of occurrence of fault modes, etc.

A.1.2.2 Application

Fault tree analysis has a two-fold application, as a means of identification of a cause of a known failure, and as a failure mode analysis and dependability modelling and prediction tool.

FTA is used to investigate potential faults, their modes and causes, and to quantify their contribution to system unavailability in the course of product design. The fault tree is constructed to represent not only system functions but also their hardware and software along with their interactions. If the human is part of the system, human errors can be included in the FTA as well. The probability of occurrence of the causes of fault modes is determined by engineering analysis, and then rolled up to evaluate the magnitude of their contribution to the overall product unreliability, allowing trade-off and reliability growth. This allows dependability modelling of mixed hardware, electronic and mechanical, and software and their interaction. In this application, the FTA becomes a powerful analysis tool.

A.1.2.3 Key elements

The key elements of a fault tree are

– gates and events,
– cut sets.

Gates represent the outcome, and events represent input into gates. Symbolic representation of some specific gates may vary from one textbook or analysis software to another; however, representation of the basic gates is fairly universal.

Cut sets are groups of events that, if all occur, would cause a system failure. Minimal cut sets contain the minimum number of events that are required for failure. A removal of one of them would result in the system not failing.

A.1.2.4 Benefits

– Can be started in early stages of a design and further developed in detail concurrently with design development.
– Identifies and records systematically the logical fault paths from a specific effect, back to the prime causes by using Boolean algebra.
– Allows easy conversion of logical models into corresponding probability measures.

A.1.2.5 Limitations

– FTA is not able to represent time or sequence dependency of events correctly.
– FTA has limitations with respect to reconfiguration or state-dependent behaviour of systems.

These limitations can compensated by combination of FTA with Markov models, where Markov models are taken as basic events in fault trees.

A.1.2.6 Example

Top level system fault tree representation for an audio amplifier: the major sub-systems are the entry gates to the top-level gate and the amplifier system.

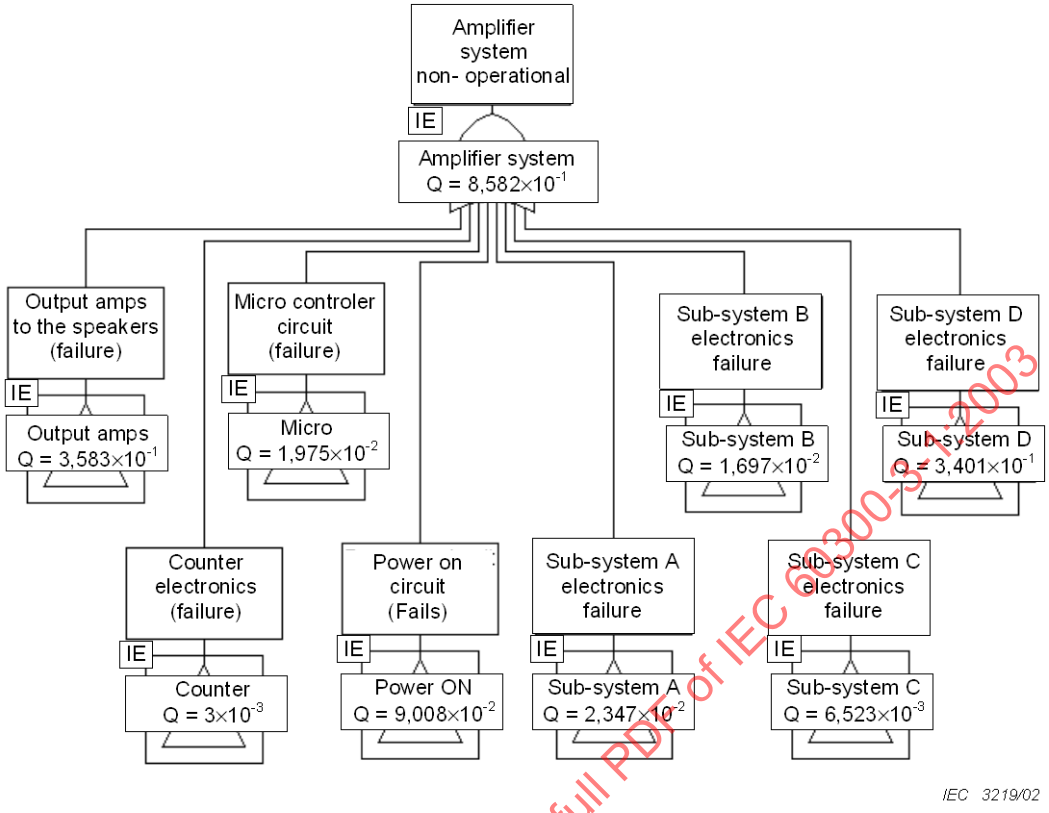


Figure A.2 – Fault tree for an audio amplifier

The highest contributor to the overall failure turned out to be the sub-tree shown in Figure A.3.

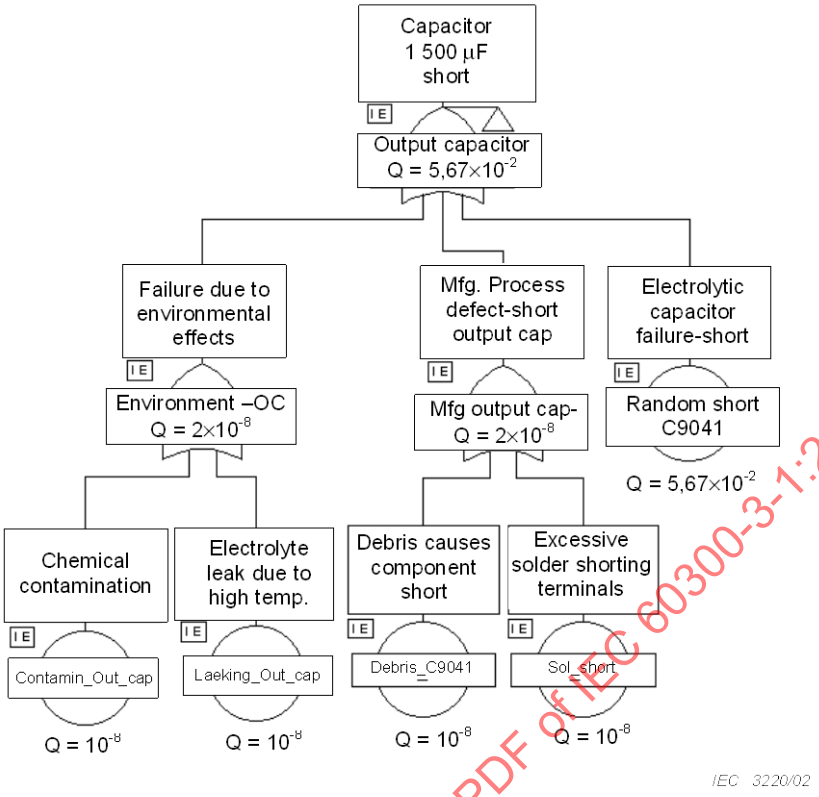
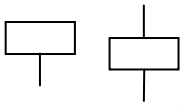


Figure A.3 – Sub-tree from FTA in Figure A.2

The symbols given in Table A.1 are used in the representation of the fault tree.

Table A.1 – Symbols used in the representation of the fault treee

FTA symbol	Symbol name	Description
	TOP EVENT or INTERMEDIATE EVENT	Top or intermediate event which describes the system fault, sub-system fault or higher level fault than the basic event level fault
	BASIC EVENT	Basic event for which reliability information is available
	UNDEVELOPED EVENT	A part of the system that yet has to be developed – defined
	TRANSFER GATE	Gate indicating that this part of the system is developed in another part or page of the diagram
	OR GATE	This output event occurs if any of its input event occurs
	AND Gate	The output event takes place if all of the input events occur

The goal of this analysis was to find the most likely cause of amplifier failure. The highest contributor to amplifier failure appears to be the electrolytic capacitor on the amplifier output to the speaker. There is a high probability that shorting of this capacitor resulting from its inherent failure rate will occur. This is due to the fact that the capacitor of lower voltage rating was originally chosen for the design because of its smaller physical size, thus the derating of this capacitor was 90 %, taking into consideration the DC voltage only. Ripple current was but an additional cause of capacitor failure.

Both causes produced an order of magnitude increase in the failure capacitor original failure rate that, for the size of the electrolytic capacitor (1 500 µF) is not low, even under higher derating. The capacitor was replaced with one with the proper voltage rating and since it appears on six places in the design, the replacement has reduced overall probability of amplifier failure for its predetermined life expectancy by more than 20 %. The result of this fault mode cause mitigation is an improvement in the system reliability.

Here, the system unavailability, Q, calculated for the given time of operation, also represents the system probability of failure, $F(t)$, as the repair times were not allowed.

The gates in the above example are standard annotations, except for the gates representing the sub-systems, where the triangle, representing the transfer gates mean that the gates were developed later, and the square around them denotes that each of those is shown on a separate page.

A.1.3 Event tree analysis (ETA)

A.1.3.1 Description and purpose

The event tree considers a number of possible consequences of an initiating event or a system failure. Thus, the event tree may be very efficiently combined with a fault tree. The root of an event tree may be viewed as the top event of a fault tree. This combination is sometimes called cause consequence analysis, where FTA is used to analyse the causes and ETA is used to analyse the consequences of an initiating event. In order to evaluate seriousness of certain consequences that follow an initiating event, all possible consequence avenues should be identified and investigated and their probability determined.

A.1.3.2 Application

Event tree analysis is used when it is essential to investigate all possible paths of consequent events, their sequence, and the most probable outcome/consequence of the initiating event. After an initiating event, there are several first subsequent events/consequences that may follow. The probability associated with occurrence of a specific path (sequence of events) represents a product of conditional probabilities of all events in that path.

A.1.3.3 Key elements

The key elements in the application of ETA are the initiator (initiating event), subsequent events, and consequences.

A.1.3.4 Benefits

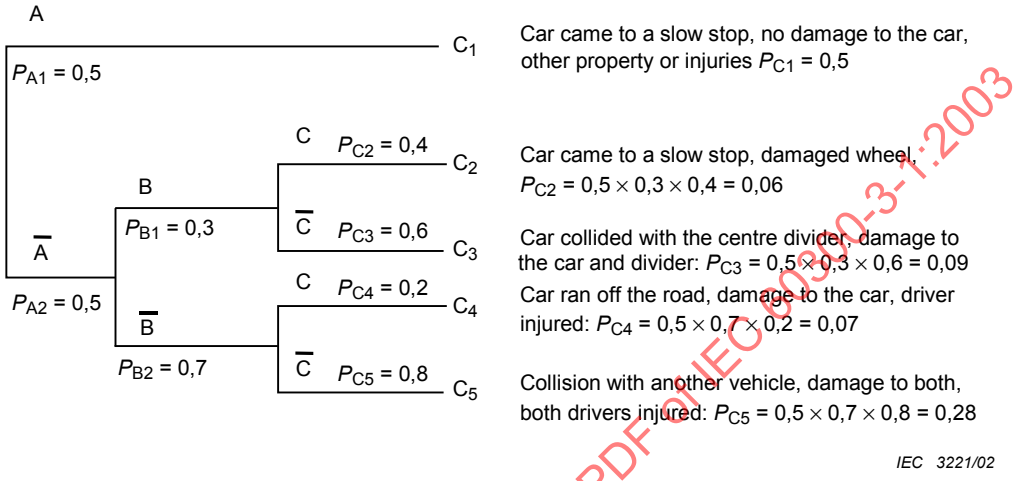
The major benefit of an event tree is the possibility to evaluate consequences of an event, and thus provide for possible mitigation of a highly probable, but unfavourable consequence. The event tree analysis is thus beneficial when performed as a complement to the fault tree analysis. The event tree analysis can also be used as a tool in the fault mode analysis. When starting bottom up, the analysis follows possible paths of an event (a failure mode) to determine probable consequences of a failure.

A.1.3.5 Limitations

Particular care has to be taken with respect to the correct handling of conditional probabilities and with respect to independence of the events in the tree analysis.

A.1.3.6 Example

An example of a simple event tree is given in Figure A.4. This example evaluates the outcome of a simple event, a car tyre failure, looking at several possible outcomes.



Key

A = no property damage or injury

B = property damage, no injury

C = damage to the car only, no other property damage

Figure A.4 – Event tree

A.1.4 Reliability block diagram analysis (RBD)

A.1.4.1 Description and purpose

Reliability block diagram (RBD) analysis is a system analysis method. An RBD is the graphical representation of a system's logical structure in terms of sub-systems and/or components. This allows the system success paths to be represented by the way in which the blocks (sub-systems/components) are logically connected.

A.1.4.2 Application

Block diagrams are among the first tasks completed during product definition. They should be constructed as part of the initial concept development. They should be started as soon as the program definition exists, completed as part of the requirements analysis, and continually expanded to a more detailed level as data become available in order to make decisions and trade-offs.

A.1.4.3 Key elements

Various qualitative analysis techniques may be employed to construct an RBD.

– Establish the definition of system success.

– Divide the system in functional blocks appropriate to the purpose of the reliability analysis. Some blocks may represent system sub-structures, which in turn may be represented by other RBDs (system reduction).

– Conduct qualitative analyses; for the quantitative evaluation of an RBD, various methods are available. Depending on the type of structure (reducible or irreducible), simple Boolean techniques, truth tables and/or path and cut set analysis may be employed for the prediction of system reliability and availability values calculated from basic component data.

A.1.4.4 Benefits

– Often constructed almost directly from the system functional diagram; this has the further advantage of reducing constructional errors and/or systematic depiction of functional paths relevant to system reliability.
– Deals with most types of system configuration including parallel, redundant, standby and alternative functional paths.
– Capable of complete analysis of variations and trade-offs with regard to changes in system performance parameters.
– Provides (in the two-state application) for fairly easy manipulation of functional (or non-functional) paths to give minimal logical models (e.g. by using Boolean algebra).
– Capable of sensitivity analysis to indicate the items dominantly contributing to overall system reliability.
– Capable of setting up models for the evaluation of overall system reliability and availability in probabilistic terms.
– Results in compact and concise diagrams for a total system.

A.1.4.5 Limitations

– Does not, in itself, provide for a specific fault analysis, i.e. the cause-effect(s) paths or the effect-cause(s) paths are not specifically highlighted.
– Requires a probabilistic model of performance for each element in the diagram.
– Will not show spurious or unintended outputs unless the analyst takes deliberate steps to this end.
– Is primarily directed towards success analysis and does not deal effectively with complex repair and maintenance strategies or general availability analysis.
– Is in general limited to non-repairable systems.

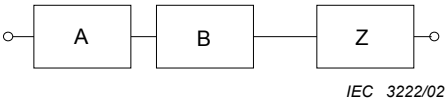
A.1.4.6 Standards

The applicable IEC standard is IEC 61078.

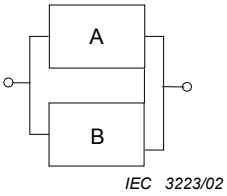
A.1.4.7 Example

Elementary models (each block should be independent of another block) are shown in Figure A.5.

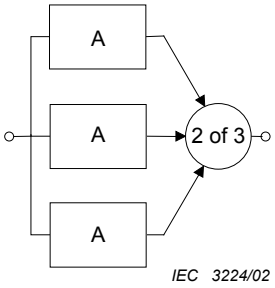
Series



Parallel (active)



Model m out of n



Standby
(cold standby)

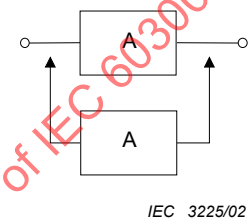


Figure A.5 – Elementary models

More complex models in which the same block appears more than once in the diagram can be assessed by the use of

– the theorem of total probability,
– Boolean truth tables.

A.1.5 Markov analysis

A.1.5.1 Description and purpose

Markov modelling is a probabilistic method that allows for the statistical dependence of the failure or repair characteristics of individual components to be adapted to the state of the system. Hence, Markov modelling can capture the effects of both order-dependent component failures and changing transition rates resulting from stress or other factors. For this reason, Markov analysis is a method suitable for the dependability evaluation of functionally complex system structures and complex repair and maintenance strategies.

The method is based on the theory of Markov chains. For dependability applications, the normal reference model is the time homogeneous Markov model that requires the transition (failure and repair) rates to be constant. At the expense of increasing the state space, non-exponential transitions may be approximated by a sequence of exponential transitions. For this model, general and efficient numerical solution techniques are available, and the only limitation to its application is the dimension of the state space.

The representation of the system behaviour by means of a Markov model requires the determination of all the possible system states, preferably shown diagrammatically in a state-transition diagram. Furthermore, the (constant) transition rates from one state to another (component failure or repair rates, event rates, etc.) have to be specified. Typical outputs of a Markov model are the probability of being in a given set of states (typically this probability is the availability performance measure).

A.1.5.2 Application

The proper field of application of this technique is when the transition (failure or repair) rates depend on the system state or vary with load, stress level, system structure (e.g. stand-by), maintenance policy or other factors. In particular, the system structure (cold or warm stand-by, spares) and the maintenance policy (single or multiple repair crews) induce dependencies that cannot be captured by other, less computationally intensive techniques.

Typical applications are reliability/availability predictions.

A.1.5.3 Key elements

The following key steps are involved in the application of the methodology:

– definition of system state space;
– assignment of (time independent) transition rates among states;
– definition of output measures (group the states that result in a system failure);
– generation of the mathematical model (transition rate matrix) and resolution of the Markov models by resorting to a suitable software package;
– analysis of results.

A.1.5.4 Benefits

Application of the methodology gives the following benefits.

– It provides a flexible probabilistic model for analysing system behaviour.
– It is adaptable to complex redundant configurations, complex maintenance policies, complex fault-error handling models (intermittent faults, fault latency, reconfiguration), degraded modes of operation and common cause failures.
– It provides probabilistic solutions for modules to be plugged into other models such as block diagrams and fault trees.
– It allows for accurate modelling of the event sequences with a specific pattern or order of occurrence.

A.1.5.5 Limitations

– As the number of system components increases, there is an exponential growth in the number of states resulting in labour intensive analysis.
– The model can be difficult for users to construct and verify, and requires specific software for the analysis.
– The numerical solution step is available only with constant transition rates.
– Specific measures, such as MTTF and MTTR, are not immediately obtained from the standard solution of the Markov model, but require direct attention.

A.1.5.6 Standards

The applicable IEC standard is IEC 61165.

A.1.5.7 Example

An electronic equipment (or unit) contains a functional (F) part and a diagnostic (D) part (see Figure A.6). By “diagnostics” is meant parts of the system which carry out all supervising, monitoring and display functions, by whatever means (hardware, software, firmware); these parts also being referred to as “supervision parts”.

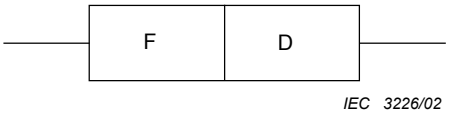


Figure A.6 – Example of unit

The following terminology is used in this example:

alarm defection
inability to raise an alarm due to a fault in the diagnostic part

down state
state of an item characterized either by a fault, or by a possible inability to perform a required function during preventive maintenance

false alarm
fault indicated by built-in test equipment or other monitoring circuitry where no functional fault exists

fault mode
one of the possible states of a faulty item, for a given required function

fault coverage
proportion of faults of an item that can be recognized under given conditions

fault diagnosis
actions taken for fault recognition, fault localization and cause identification

latent fault
existing fault that has not yet been recognized

up state
state of an item characterized by the fact that it can perform a required function, assuming that the external resources, if required, are provided

Reliability models usually involve some simplifications: in a block diagram each functional block has two states. One state means correct operation (up state) and the other means fault (down state). The two-state model greatly simplifies reliability analysis, but sometimes it is not adequate to describe what happens in the real world in which each functional block has to have a functional (F) part and a diagnostic (D) part and both can fail: Markov modelling allows to deal with these issues.

The application of Markov analysis first requires the definition of the system state space. Table A.2 and Table A.3 show the states of a real world unit and the effects of failures in the F and D states.

Table A.2 – States of the unit

State	Definition
1	Correct operation
2	Diagnostic fault in alarm defection mode
3	Functional fault covered by diagnostics
4	Functional fault not covered by diagnostics (not detectable)
5	Functional fault not detected by diagnostics failed in alarm defection mode
6	Diagnostic fault in false alarm mode

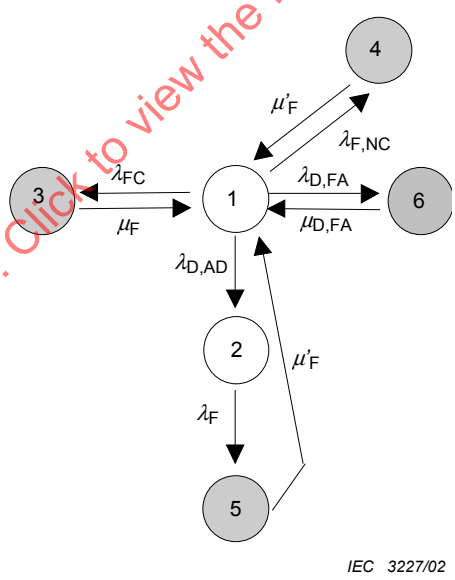
Table A.3 – Effects of failures in functional and diagnostic parts

State of F	State of D	State	Effects
Operating	Operating	1	Correct operation (state 1)
Operating	Fault in false alarm mode	6	Alarm emitted. F is in up state until maintenance personnel perform a repair action. In general, if F is not redundant, the system normally leaves it in service (state 6) until the repair action takes place
	Fault in alarm defection mode	2	No alarm emitted. F part is in the up state (state 2) until it fails (state 5)
Fault	Operating	3	Alarm emitted. Correct fault recognition (state 3)
Fault	Fault	5	Sequence of events to arrive in this state: Diagnostic fault (alarm defection mode), sub-system goes into state 2 Functional fault; no alarm emitted (state 5)
Fault	Missing	4	Undetectable fault (state 4)

Figure A.7 shows the associated state-transition diagram and admits that

– the functional part may not be covered by diagnostics; this means that a failure in the functional part might not be detected (State 4),

– the diagnostics may fail to emit an alarm when they should not (State 6) or may not emit an alarm when they should (States 2 and 5).



NOTE White encircled states are up states while grey encircled states are down states.

Figure A.7 – State-transition diagram

The (time independent) transition rates among states are shown in Table A.4.

Table A.4 – Transition rates

λ_F	Failure rate of F, the functional part
$\lambda_{F,C}$	Covered failure rate of F (failures detectable by diagnostics)
$\lambda_{F,NC}$	Uncovered failure rate of F (note that $\lambda_F = \lambda_{F,C} + \lambda_{F,NC}$)
$\lambda_{D,AD}$	Failure rate of D in alarm defection mode
$\lambda_{D,FA}$	Failure rate of D in false alarm mode (note that $\lambda_D = \lambda_{D,AD} + \lambda_{D,FA}$)
μ_F	Repair rate after a covered fault
μ'_F	Repair rate after an uncovered fault
$\mu_{D/FA}$	Repair rate after a fault in false alarm mode

Once the states diagram and the transition rates have been defined, availability can be calculated by using a suitable software package. It is also quite easy to perform a parametric analysis, considering variations of the transition rates.

A.1.6 Petri net analysis

A.1.6.1 Description and purpose

Petri nets are a graphical tool for the representation and analysis of complex logical interactions among components or events in a system. Typical complex interactions that are naturally included in the Petri net language are concurrency, conflict, synchronization, mutual exclusion and resource limitation.

The static structure of the modelled system is represented by a Petri net graph. The Petri net graph is composed of three primitive elements:

– places (usually drawn as circles) that represent the conditions in which the system can be found;

– transitions (usually drawn as bars) that represent the events that may change a condition in to another one;

– arcs (drawn as arrows) that connect places to transitions and transition to places and represent the logical admissible connections between conditions and events.

A condition is valid in a given situation if the corresponding place is marked, i.e. contains at least one token • (drawn as a black dot). The dynamics of the system are represented by means of the movement of the tokens in the graph. A transition is enabled if its input places contain at least one token. An enabled transition may fire, and the transition firing removes one token from each input place and puts one token into each output place. The distribution of the tokens into the places is called the marking. Starting from an initial marking, the application of the enabling and firing rules produces all the reachable markings called the reachability set of the Petri nets. The reachability set provides all the states that the system can reach from an initial state.

Standard Petri nets do not carry the notion of time. However, many extensions have appeared in which a timing is superimposed onto the Petri net. If a (constant) firing rate is assigned to each transition, the dynamics of the Petri nets can be analysed by means of a continuous Markov time chain whose state space is isomorphic with the reachability set of the corresponding Petri net.

The Petri net can be utilized as a high level language to generate Markov models, and several tools in performance dependability analysis are based on this methodology.

Petri nets provide also a natural environment for simulation.

A.1.6.2 Application

The use of Petri nets is recommended when complex logical interactions need to be taken into account (concurrency, conflict, synchronization, mutual exclusion, resource limitation). Moreover, Petri nets are usually an easier and more natural language to describe a Markov model.

A.1.6.3 Key elements

The key element of the Petri net analysis is a description of the system structure and its dynamic behaviour in terms of primitive elements (places, transitions, arcs and tokens) of the Petri net language; this step requires the use of ad hoc software tools:

a) structural qualitative analysis;

b) quantitative analysis: if constant firing rates are assigned to the Petri net transitions the quantitative analysis can be performed via the numerical solution of the corresponding Markov model, otherwise simulation is the only viable technique.

A.1.6.4 Benefits

Petri nets are suitable for representing complex interactions among hardware or software modules that are not easily modelled by other techniques.

Petri nets are a viable vehicle to generate Markov models. In general, the description of the system by means of a Petri net requires far fewer elements than the corresponding Markov representation.

The Markov model is generated automatically from the Petri net representation and the complexity of the analytical solution procedure is hidden to the modeller who interacts only at the Petri net level.

In addition, the Petri nets allow a qualitative structural analysis based only on the property of the graph. This structural analysis is, in general, less costly than the generation of the Markov model, and provides information useful to validate the consistency of the model.

A.1.6.5 Limitations

Since the quantitative analysis is based on the generation and solution of the corresponding Markov model, most of the limitations are shared with the Markov analysis.

The Petri net methodology requires the use of software tools (several are available, developed by academic and industrial bodies).

A.1.6.6 Example

A fault-tolerant multiprocessor computer system, whose block diagram is depicted in Figure A.8, contains two independent sub-systems S_1 and S_2 with a shared common memory M_3.

Each sub-system S_i (i = 1; 2) is composed of one processor P_i, one local memory M_i and two replicated disk units D_{i1} and D_{i2}. A single bus N connects the two sub-systems and the shared common memory.

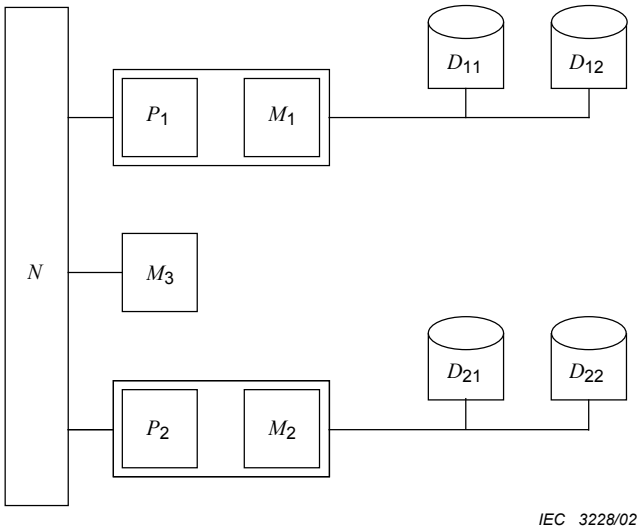


Figure A.8 – Block diagram of a multiprocessor system

The GSPN (generalized stochastic Petri net) representation of the system of Figure A.8 is depicted in Figure A.9.

Places whose names have the suffix *.dn* model components in the non-operational condition.

A token in place S.*dn* models the overall system failure.

Transitions whose names have the suffix *.f* model the failure of a component.

The initial marking of the net represents the multiprocessor having all components operational.

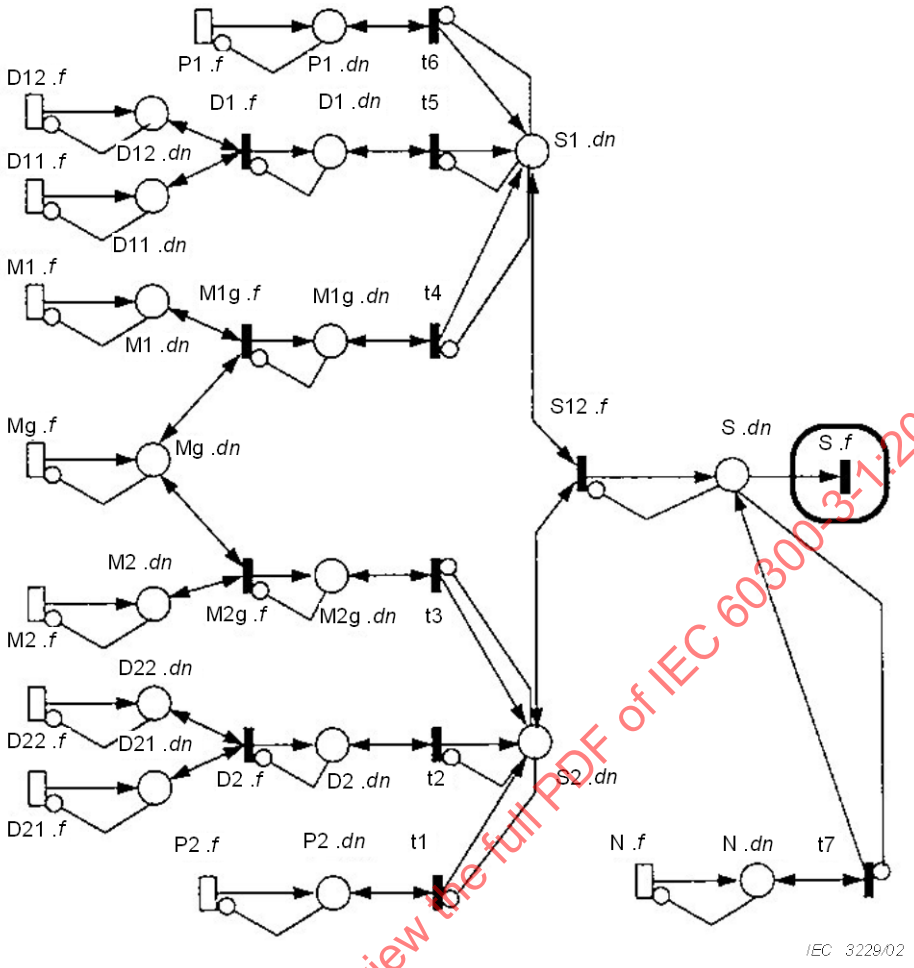


Figure A.9 – Petri net of a multiprocessor system

A.1.7 Failure modes and effects analysis (FMEA)

A.1.7.1 Description and purpose

Failure modes and effects analysis (FMEA) is a bottom-up, qualitative dependability analysis method, which is particularly suited to the study of material, component and equipment failures and their effects on the next highest functional system level. Iterations of this step (identification of single failure modes and the evaluation of their effects on the next highest system level) result in the eventual identification of all the system single failure modes. FMEA lends itself to the analysis of systems of different technologies (electrical, mechanical, hydraulic, software, etc.) with simple functional structures. Failure modes, effects and criticality analysis (FMECA) extends the FMEA to include criticality analysis by quantifying failure effects in terms of probability of occurrence and the severity of any effects. The severity of effects is assessed by reference to a specified scale.

A.1.7.2 Application

FMEAs or FMECAs are generally carried out where a level of risk is anticipated in a program early in product or process development. Factors that may be considered are new technology, new processes, new designs, or changes in the environment, loads, or regulations. FMEAs or FMECAs can be effected on components or systems that make up products, processes or manufacturing equipment. They can also be carried out on software systems.

A.1.7.3 Key elements

The FMEA or FMECA analysis generally follows the following steps:

– identification of how the component of system should perform;
– identification of potential failure modes, effects and causes;
– identification of risk related to failure modes and its effects;
– identification of recommended actions to eliminate or reduce the risk;
– follow-up actions to close out the recommended actions.

A.1.7.4 Benefits

– Identifies systematically the cause and effect relationships.
– Gives an initial indication of those failure modes that are likely to be critical, especially single failures that may propagate.
– Identifies outcomes arising from specific causes or initiating events that are believed to be important.
– Provides a framework for identification of measures to mitigate risk.
– Useful in the preliminary analysis of new or untried systems or processes.

A.1.7.5 Limitations

– The output data may be large even for relatively simple systems.
– May become complicated and unmanageable unless there is a fairly direct (or “single-chain”) relationship between cause and effect.
– May not easily deal with time sequences, restoration processes, environmental conditions, maintenance aspects, etc.
– Prioritizing mode criticality is complicated by competing factors involved.

A.1.7.6 Standards

The applicable IEC standard is IEC 60812.

A.1.7.7 Example

An example of failure mode and effects analysis is given in Table A.5.

Table A.5 – Example of FMEA

Indenture level:					**Design by:**				**Prepared by:**			
Sheet No.:					**Item:**				**Approved by:**			
Mission phase					**Issue:**				**Date:**			
Item ref.	**Item description / function**	**Failure entry code**	**Failure mode**	**Possible failure causes**	**Symptom detected by**	**Local effect**	**Effect on unit output**	**Compensating provision against failure**	**Severity class**	**Failure rate**	**Data source**	**Recommendations and actions taken**
1.1.1	Motor stator	1111	Open circuit	Winding fracture	Low speed roughness	Low power	Trip	Single phase protection temperature trip	4			
		1112	Open circuit	Connection fracture	Low speed roughness	Low power	Trip	Single phase protection temperature trip	3			
		1113	Isolation breakdown	Persistent high temp. manufactur-ing defect	Protection system	Overload	No output	Annual inspection temperature trip	4			
		1114	Thermistor open circuit	Ageing; connection fracture	Protection system	None	No output	Fitted spare	3			Recommend a spare connected through to outside casing
		1115	Thermistor short cut	Protection system	Protection system	Reduced trip margin	No output if load is high	Fitted spare temperature trip	3			Recommend a spare connected through to outside casing
1.1.2	Motor cooling system	1121	Inadequate cooling	Blockage low diff. pressure	High temperature stator detected by thermistor	Excessive winding temperature	Excessive motor temperature	Temperature trip stator	2			
		1122	Leakage to atmosphere	Piping connection	Motor temperature	Motor, inadequate cooling	Excessive motor temperature	Temperature trip, check every 2 h	2			
		1122	Leakage from atmosphere	Piping connection	Low output	Air in system	None	Check every 2 h	2			
1.1.3	Motor bearing	1131	Seal external leakage	Wear bearing failure	Low level lub oil sump	Loss of lub oil	None unless leak severe	Daily check	3			

A.1.8 Hazard and operability studies (HAZOP)

A.1.8.1 Description and purpose

A HAZOP study is a detailed hazard and operability problem identification process, carried out by a team. HAZOP deals with the identification of potential deviations from the design intent, examination of their possible causes and assessment of their consequences.

The basis of HAZOP is a "guide word examination" which is a deliberate search for deviations from the design intent. The design intent is the designer's desired, or specified, behaviour for a system, its elements and characteristics. To facilitate the examination, a system is divided into parts in such a way that the design intent for each part can be adequately defined. The design intent for a given part of a system is expressed in terms of elements which convey the essential features of the part and which represent natural divisions of the part. Elements may be discrete steps or stages in a procedure, individual signals and equipment items in a control system, equipment or components in a process or electronic system, etc.

The identification of deviations from the design intent is achieved by a questioning process using predetermined "guide words". The role of the guide word is to stimulate imaginative thinking, to focus the study and elicit ideas and discussion, thereby maximizing the chances of study completeness. Guide words and their meanings are given in Tables A.6 and A.7.

Table A.6 – Basic guide words and their generic meanings

Guide word	Meaning
No or Not	Complete negation of the design intent
More	Quantitative increase
Less	Quantitative decrease
As well as	Qualitative modification/increase
Part of	Qualitative modification/decrease
Reverse	Logical opposite of the design intent
Other than	Complete substitution

Table A.7 – Additional guide words relating to clock time and order or sequence

Guide word	Meaning
Early	Relative to the clock time
Late	Relative to the clock time
Before	Relating to order or sequence
After	Relating to order or sequence

A.1.8.2 Application

HAZOP is most suitable in the later stages of detailed design for examining operating facilities, and when changes to existing facilities are made. The best time to carry out a HAZOP study is just before the design is frozen.

A.1.8.3 Key elements

– The examination is a creative process.

– The examination proceeds by systematically using a series of guide words to identify potential deviations from the design intent and employing these deviations as "triggering

devices" to stimulate team members to envisage how the deviation might occur and what might be the consequences.

– The examination is carried out under the guidance of a trained and experienced study leader, who has to ensure comprehensive coverage of the system under study, using logical, analytical thinking.
– The examination relies on specialists from various disciplines with appropriate skills and experience who display intuition and good judgement.
– The examination should be carried out in a climate of positive thinking and frank discussion. When a problem is identified, it is recorded for subsequent assessment and resolution.
– Solutions to identified problems are not a primary objective of the HAZOP examination, but if made they are recorded for consideration by those responsible for the design.

HAZOP studies consist of four basic sequential steps, shown in Figure A.10.

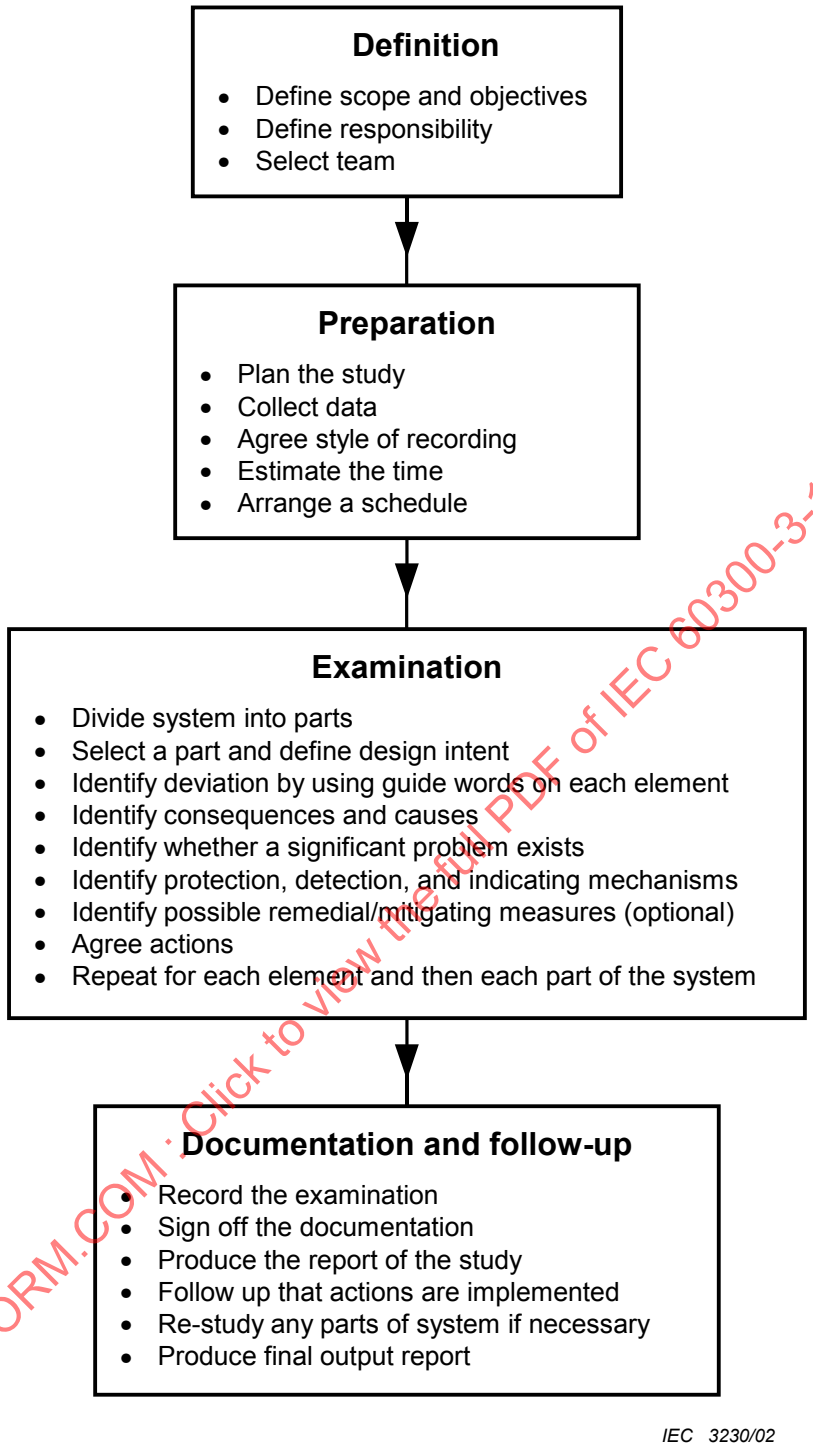


Figure A.10 – The HAZOP study procedure

A.1.8.4 Benefits

– Utilizes the various skills and knowledge of a group of experts, each familiar with a different aspect of the system under study.

– Efficient in finding both causes and consequences of deviations at various levels in the system.

– Suitable for reviews of processes which can be described by a flow-diagram.

– Resulting knowledge is of great assistance in determining appropriate remedial measures.

A.1.8.5 Limitations

Whilst HAZOP studies have proved to be extremely useful in a variety of different industries, the technique has limitations that should be taken into account when considering a potential application.

– HAZOP is a hazard identification technique which considers system parts individually and methodically examines the effects of deviations on each part. Sometimes a serious hazard will involve the interaction between a number of parts of the system. In these cases the hazard may need to be studied in more detail using techniques such as event tree and fault tree analyses.

– As with any technique for the identification of hazards or operability problems, there can be no guarantee that all hazards or operability problems will be identified in a HAZOP study. The study of a complex system should not, therefore, depend entirely upon HAZOP. It should be used in conjunction with other suitable techniques (e.g. fault tree analysis).

– Many systems are highly inter-linked, and a deviation at one of them may have a cause elsewhere. Adequate local mitigating action may not address the real cause and still result in a subsequent accident.

– The success of a HAZOP study depends greatly on the ability and experience of the study leader and the knowledge, experience and interaction between team members.

– HAZOP only considers parts, their elements and characteristics that appear on the design representation. Activities and operations which do not appear on the representation are not considered.

A.1.8.6 Standards

The applicable IEC standard is IEC 61882.

A.1.9 Human reliability analysis (HRA)

A.1.9.1 Description and purpose

Human reliability analysis is a subtask of the more general human factor analysis, which is a collective name for the allocation of functions, tasks and resources among humans and machines and the assessment of human reliability. Human factor analysis is not a discipline on its own; rather, it is an activity that engages the application of various disciplines to the problem area where humans and machines should reliably perform. It embodies the disciplines of psychology, physiology, sociology, medicine and engineering.

A particular purpose of human factor analysis is to assess factors that may impact human reliability in the operation of a system; often referred to as the human reliability analysis. Reliable human performance is necessary for the success of human/machine systems and is influenced by many factors. These factors may be internal such as stress, emotional state, training, motivation and experience, or external, such as work hours, environment, actions by supervisors, procedures and hardware interfaces.

A.1.9.2 Application

The most effective application of the human factor perspective is by its active involvement in all phases of system development from design to training, operation and disposal. Its focus ranges from overall system considerations (including operational management) to the interaction of a single individual at the lowest operational level.

In principle any task performed by the human represents an opportunity for human error; that is, each of these tasks should be reliably performed. After identifying those tasks, each one is analysed to identify any error likely situations that may cause the operator to fail. This may be compared to a kind of FMEA for human tasks.

Often these tasks are assessed by creating event trees for each one. The event tree conveys the task analysis information and determines a scheme to quantitatively assess the combination of failures.

A.1.9.3 Key elements

The following are typical elements in a human reliability analysis:

– description of personnel, the work environment and the tasks performed;
– analysis of human/machine interfaces;
– performance of task analysis of intended operator functions;
– performance of human error analysis of intended operator function;
– documentation of results.

A.1.9.4 Benefits

The analysis of mishaps and accidents shows that reliable human performance is a key factor for the dependability of human/machine systems. If human factors are disregarded, the dependability predictions for a system may be completely misleading. Human reliability analysis contributes to the usability of the product.

A.1.9.5 Limitations

Application of human reliability analysis to a system requires an in-depth knowledge of human performance parameters.

In particular, if historical data are not available, the quantitative analysis may have to rely on subjective estimation of human error probabilities.

Human factor analysis is often not regarded as a part of reliability engineering and it is sometimes hard to convince project managers to start a human factor analysis or human reliability analysis at all.

A.1.9.6 Example

In an application where a key is used to start up a system, for example, a train, the key shall be replaced by an electronic smart card (for whatever reason). This solution is used in several variations of automated teller machines (ATM). The (relative) impact of this change on the availability of the system (with respect to the former solution) shall be estimated.

Step 1: Consider a driver in a railway-specific work environment and his interaction with the system at start-up of a train. His tasks are to enter his smart card and a PIN code to authenticate himself.

Step 2: The interface is well known from ATM. It consists of a smart card reader, a display and a numeric pad to enter the PIN.

Step 3: Task 1 is defined as entering the smart card. Task 2 is defined as entering the correct PIN.

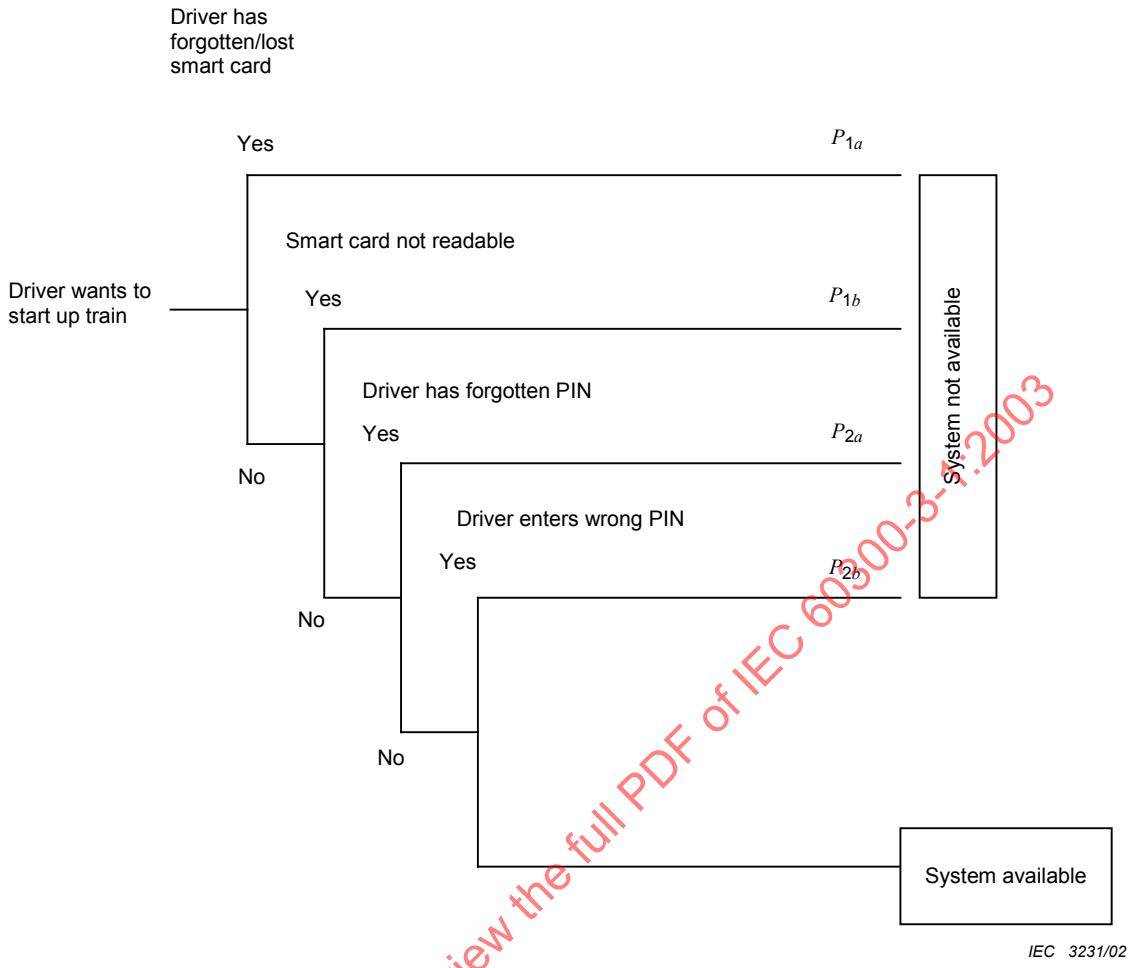
Step 4: Credible human errors could be those given in Table A.8 (not necessarily exhaustive)

Table A.8 – Credible human errors

Task	Human error	Cause	Measures
a)	1) The driver has forgotten or lost the smart card	i) Improper means for storing the card	Supply suitable means of storage or casing for the card that is accepted by the driver
		ii) Inattentiveness	Implement checks that ensure (say at the beginning of the workday) that this has no operational effect. Supply wildcards for such a case
	2) The smart card is in a condition that renders it not readable by the system	i) Improper means for storing the card	As above
		ii) Improper handling	Training with respect to handling of smart cards. Regular checks. Contactless smart cards as an alternative design (cost-effectiveness to be checked)
b)	1) The driver has forgotten the PIN	Forgetfulness	Training. As a design alternative the driver might choose the PIN by himself (a number that is easier to remember) instead of being assigned a PIN by the system
	2) The driver enters an incorrect PIN	Typing error, etc.	Allow at least one repeat. Design the numeric pad ergonomically in order to minimize type errors (e.g. keys should not be too small, easily readable, give an acknowledgement (beep) when a number is pushed, etc.)

This information can also be represented in an event tree (see Figure A.11).

The event tree can be quantified by assigning probabilities to each branch. However, even in this small example, obtaining accurate data or models may not be that straightforward. While some data can be collected from ATM applications it should be remembered that the work environment encountered here might be completely different. In this example, the unavailability is merely the sum of all mentioned probabilities in the event tree. For the sake of the example, only hypothetical values are given.



Parameter	Value	Remark
P_{1a}	10^{-4}	Drivers are known to be careful, trained to handle smart cards such as keys, proper storage ensured, checks implemented
P_{1b}	10^{-4}	Proper casing for smart cards
P_{2a}	10^{-4}	Drivers have been allowed to choose their PIN, they are aware of the consequences, e.g. train delays
P_{2b}	10^{-2}	Ergonomically designed numeric pad, but typing errors may always occur

Figure A.11 – Human errors shown as an event tree

The result is that the unavailability is poor, about 0,01 per journey, which is unacceptable. As a remedy, the driver is allowed a second try to enter the PIN after an error. The probability of failing twice is $P_{2b} \times P_{2b} = 10^{-4}$ in this example, thus giving an estimated total unavailability of 0,0004 per journey (four out of 10 000 trains will be delayed), which seems acceptable. Allowing more trials might bring the unavailability down to 0,0003, but may be unacceptable from a security point of view.

A.1.10 Stress-strength analysis

A.1.10.1 Description and purpose

The stress-strength analysis is a method to determine capability of a component or an item to withstand electrical, mechanical, environmental, or other stresses that might be a cause of their failure. This analysis determines the physical effect of stresses on a component, as well as the mechanical or physical ability of the component. Probability of component failure is directly proportional to the applied stresses. The specific relationship of stresses versus component strength determines component reliability.

A.1.10.2 Application

Stress-strength analysis is primarily used in determination of reliability or equivalent failure rate of mechanical components. It is also used in physics of failure to determine likelihood of occurrence of a specific failure mode due to a specific individual cause in a component.

Component structural reliability, i.e. its capability to withstand electrical or other stresses, depends on its strength or load-carrying capability, where reliability is the probabilistic measure of assurance of the component performance. Determination of this load-carrying capability involves uncertainty; therefore, this capability is modelled as a random variable, as opposed to the applied stress which, for the same reason of uncertainty, is modelled as another random variable. The overlap of these random variables, when represented by a distribution, represents the degree of probability that the stress will exceed the strength, that is, the area of overlap of the respective probability density functions represents probability of failure occurrence.

Evaluation of stress against strength and resultant reliability of parts depends upon evaluation of the second moments, the mean values and variances of the expected stress and strength random variables. This evaluation is often simplified to one stress variable compared to strength of the component.

In general terms, the strength and stress shall be represented by the performance function or the state function, which is a representative of a multitude of design variables including capabilities and stresses. Positive value of this function represents the safe state while negative value represents the failure state.

A.1.10.3 Key elements

The key elements include a detailed knowledge of the component materials and construction, as well as other properties of interest as well as proper modelling of expected stresses.

A.1.10.4 Benefits

Stress-strength analysis can provide accurate representation of component reliability as a function of the expected failure mechanisms. It includes variability of design as well as variability of expected applied stresses, and their mutual correlation. In this sense, the technique provides a more realistic insight into effects of multiple stresses and is more representative of physics of component failure, as many factors – environmental and mechanical – can be considered, including their mutual interaction.

A.1.10.5 Limitations

In the case of multiple stresses, and especially when there is an interaction or correlation between two or more stresses present, the mathematics of problem solving can become very involved, requiring professional mathematical computer tools. Another disadvantage is possible wrong assumption on distribution of one or more random variables, which, in turn, can lead to erroneous conclusions.

A.1.10.6 Example

A simple example of application of stress–strength criteria is application of force on an O-ring where the failure criterion was its leak. To calculate probability of occurrence of this failure, a mean force necessary to produce the leak, F_0, was calculated based on the O-ring inner and outer dimensions, its geometry, and material properties – this was deemed as the strength. Both, strength and the applied force, F, were assumed to be normally distributed, with the respective standard deviations equal to one-tenth of the respective mean values. Probability of failure was calculated as:

$$P_F = \Phi\left[\frac{F - F_0}{\sqrt{\sigma_F^2 + \sigma_{F_0}^2}}\right] = 1{,}9 \times 10^{-6}$$

Figure A.12 represents this example.

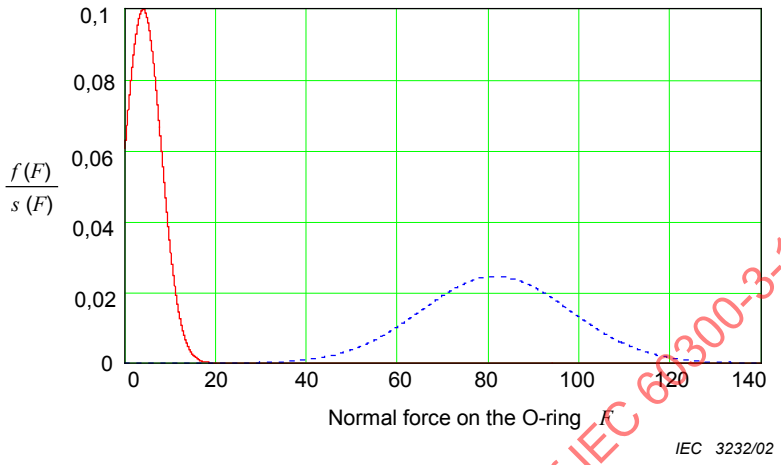


Figure A.12 – Example – Application of stress–strength criteria

A.1.11 Truth table

A.1.11.1 Description and purpose

The mathematical qualities of the truth table method (TTM) – also called structure function analysis – are widely appreciated in certain fields, in particular in the electrical engineering and electronics areas. The method consists of listing all possible state combinations (operating state, failed state) for the various components that make up a system and studying their effects.

A.1.11.2 Application

The first steps in the application of the method are similar to those of a FMECA. The failure modes of the components as well as their failed states should be listed once the system has been broken down into a manageable size. Generally each component is characterized by an operating state and a failed state. The definition of a state vector is thus a combination of component states, each component being represented by either its operating state or its failed state.

The truth table is worked out by analysing the effects of all the component state vectors. All the failures of the system are thus identified. The results are then summarized in a table called the 'truth table', where "0" is the operating state and "1" the failed state. The study of each state vector should also include a failure (or fault) analysis in order to find out the likely common failure causes.

The probability of the system failed state is worked out by calculating the occurrence probability of each state vector resulting in the system failed state. This can be done since the vector states are disconnected when the components are independent. Figure A.13 shows a truth table for some simple systems.

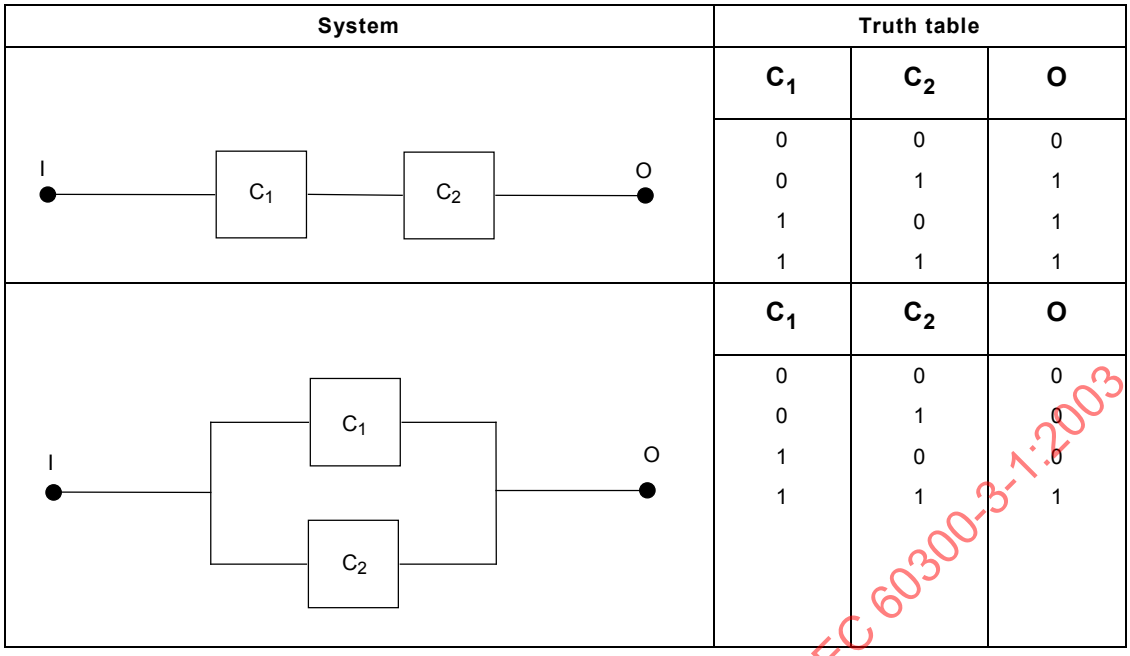


Figure A.13 – Truth table for simple systems

The TTM entails the study of all the possible combinations of the component operating and failed states. It is thus, in theory, the most rigorous method to date. To obtain the relevant combinations, the truth table can be reduced by a Boolean method. It can be difficult to apply the method to a complex system since the number of states can quickly become very large and hence be difficult to deal with.

A.1.11.3 Standards

The method is covered in Clause 8 of IEC 61078.

A.1.11.4 Example

A system layout consists of a main signal path (K) and an alternative path (E). The alternative path does not operate in functional redundancy but under operation load. The switch (U) is not in the signal path. Determine the availability of the system.

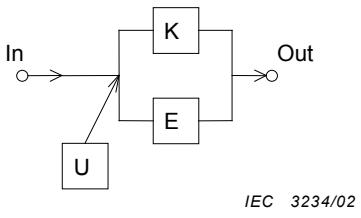


Figure A.14 – Example

The following truth table results, where 0 is the operating state and 1 the failed state:

Table A.9 – Truth table example

State	K	E	U	$P(S \mid A_i)$	$P(A_i)$	$P(S \mid A_i) \times P(A_i)$
A_1	0	0	0	1	$a_K \times a_E \times a_U$	$1 \times a_K \times a_E \times a_U$
A_2	0	1	0	1	$a_K \times (1-a_E) \times a_U$	$1 \times a_K \times (1-a_E) \times a_U$
A_3	1	0	0	1	$(1-a_K) \times a_E \times a_U$	$1 \times (1-a_K) \times a_E \times a_U$
A_4	1	1	0	0	$(1-a_K) \times (1-a_E) \times a_U$	0
A_5	0	0	1	1	$a_K \times a_E \times (1-a_U)$	$1 \times a_K \times a_E \times (1-a_U)$
A_6	0	1	1	1	$a_K \times (1-a_E) \times (1-a_U)$	$1 \times a_K \times (1-a_E) \times (1-a_U)$
A_7	1	0	1	0,5	$(1-a_K) \times a_E \times (1-a_U)$	$0,5 \times (1-a_K) \times a_E \times (1-a_U)$
A_8	1	1	1	0	$(1-a_K) \times (1-a_E) \times (1-a_U)$	0
NOTE In state A_7 the function of the system depends whether the switch is in position (K) or (E). Therefore the probability is assumed as 0,5 that the system operates in this state.						

If the random events A_1, ..., A_n exclude each other in pairs, the probability P_S follows by the theorem of total probability:

$$P_S = \sum_{i=1}^{n} P(S \mid A_i) \times P(A_i)$$

where

$P(S \mid A_i)$ is the probability that the system operates in state A_1,

$P(A_i)$ probability that the system is in state A_1.

By setting availabilities a for probabilities P, one obtains:

$$P_S = a_S = [a_K \times a_E \times a_U] + [a_K \times (1-a_E) \times a_U] + [(1-a_K) \times a_E \times a_U] + [a_K \times a_E \times (1-a_U)] + [a_K \times (1-a_E) \times (1-a_U)] + [0,5 \times (1-a_K) \times a_E \times (1-a_U)]$$

This results in

$$a_S = a_K + 0,5 \times (1-a_K) \times a_E \times (1-a_U).$$

A.1.12 Statistical reliability methods

A.1.12.1 Description and purpose

Reliability is an aspect of engineering uncertainty that may be quantified as a probability. The need to measure and manage uncertainty in reliability analysis involves the use of statistical methods.

Statistical methods are used to quantify reliability for a number of reasons including:

– estimating and predicting product reliability;

– assessing characteristics of materials over a warranty period or over the product's design life;

– predicting warranty costs;
– assessing the effect of a proposed design change;
– assessing whether customer requirements and government regulations have been met;
– tracking the product in the field to provide information on causes of failure and methods of improving product reliability;
– comparing components from two or more different manufacturers, material, production periods, operating environments, etc.

To apply any statistical methods, data have to be gathered. These data are dependent on the problem to be solved and the type of analyses to be performed. Data used for reliability analysis aim to capture information about the performance of items exposed to risk (e.g. within an operating environment). The data types will vary depending upon the type of item under investigation. For example, the basic data for one-shot devices are the number of trials and the number of successful operations; the basic data for non-repaired items are the times to events for items in the population at risk while the basic data for a repaired item are the accumulated times to events throughout the item lifetime. Usually not all items at risk will fail during the observation period. Therefore the time to failure events are recorded only for those items that fail and the running times are recorded for those items that do not fail. These so-called censoring structures can be quite complex and will depend upon the aims of the reliability study and the item of interest.

In addition to the basic data, information can be captured about factors influencing reliability and included in statistical analysis to measure their impact on performance.

IEC 60300-3-2 provides guidance on the collection of dependability data from the field. IEC 60300-3-5 provides guidance on reliability test conditions and statistical test principles.

Classical statistical methods use only the quantitative data about events as described above. However reliability data from past experience or tests may be limited but it is still necessary to have some statistical measure of reliability. For this reason, judgmental data may be collected and combined with quantitative data to produce reliability estimates using Bayesian methods.

Bayesian methods allow data from different sources to be combined in order to estimate reliability. They involve setting up a model for reliability and then using the available data to formulate a prior distribution. The prior distribution is a probability distribution that represents the uncertainty in the parameters of the model or in the reliability prior to collecting observations about reliability. The prior distribution should capture all available data, e.g. historical data on the in–service reliability of items, data on the capabilities of manufacturing processes and data on the perceived effectiveness of tests. The data used may prove to serve as subjective engineering judgement. Combining all data into a single prior distribution can prove a difficult task.

Bayesian methods provide a framework in which reliability estimates can be updated as new data becomes available. The prior distribution is combined with the original reliability model to produce a posterior distribution, from which an updated reliability estimate is given. For example, an initial reliability estimate during design might be updated during development as test data becomes available. The uncertainty in the estimates can be quantified to give upper and/or lower bounds on the reliability.

Bayesian methods can be used to combine data from different levels of equipment, for example, module and component level.

A.1.12.2 Application

The reliability models used vary according to the application, e.g. lifetime distributions such as the exponential, Weibull; stochastic processes such as the power law model; reliability growth models; degradation models; maintenance models and many more.

Each type of model can be estimated using classical or Bayesian methods. Both provide estimates of reliability, including uncertainty bands.

A.1.12.3 Key elements

Classical statistical reliability methods generally consist of the following steps:

– identification of the reliability model to be used for the problem under consideration;
– identification of the data required to provide information about the parameters of the reliability model;
– collection of relevant event data;
– estimation of the statistical model using classical methods;
– extraction of relevant reliability estimates from the model;
– repetition of the above steps when the reliability estimate is to be updated.

Bayesian reliability methods generally consist of the following steps:

– identification of the reliability model to be used for the problem under consideration;
– identification of the data required to provide information about the parameters of the reliability model;
– combination of subjective judgement into the relevant prior distribution;
– combination of the prior distribution with the model to produce the posterior distribution;
– extraction of relevant reliability estimates from the posterior distribution;
– repetition of the above steps when the reliability estimate is to be updated.

A.1.12.4 Benefits

The benefits of all statistical methods are that

– data from a variety of sources can be combined,
– estimates of reliability, with uncertainty, can be provided,
– reliability estimates can be updated as more data becomes available.

And in addition for Bayesian methods

– subjective engineering data can be combined with historical failure data,
– early estimates of reliability can be provided even when few events have been observed.

A.1.12.5 Limitations

For all statistical methods the difficulties involve

– specifying an appropriate model that is functional and will provide useful to decision-makers,
– structuring event data to be used in analysis.

And in addition for Bayesian methods

– eliciting engineering judgement can be difficult,
– constructing a prior distribution can prove a difficult task,
– calculating the updated reliability (posterior distribution) may not be straightforward.

A.2 Selected supporting methods

A.2.1 Sneak circuit analysis

A.2.1.1 Description and purpose

Sneak circuit analysis (SCA) is a computerized approach to find the sneak circuits which is defined as a latent path causing unwanted function or inhibiting a desired function without regard to part failures. The path can consist of wires, parts, software interfaces and energy sources. There are six types of latent failure conditions associated with the sneak circuit:

– sneak labels;
– sneak indicators;
– drawing errors;
– sneak paths;
– sneak timing;
– design concerns.

A.2.1.2 Application

Sneak circuit analysis is used in uncovering latent circuit conditions which result in unplanned modes of operation. SCA is widely used in aerospace systems, space development and atomic/power plant industries.

A.2.1.3 Key elements

SCA consists of the following steps:

– examination of circuits (or functions);
– searching for unintended paths.

A.2.1.4 Benefits

SCA reduces design errors and human errors in the system.

A.2.1.5 Limitations

– Few specialists handle the sneak circuit analysis based on the specific software.
– Large-scale computer systems are required.

A.2.2 Worst case analysis (WCA)

A.2.2.1 Description and purpose

The worst case analysis (WCA) is a non-statistical approach used to confirm and determine whether the system performance can fall within specifications or not under all the combinations of given tolerance limits of the system parameters.

A.2.2.2 Application

WCA is generally used for the system composed of several components and mostly during the design and development phase. For example, any designed mechanism, circuit, or network can be considered as the system. The component performance characteristics, like the system parameters, can affect the system performance characteristics and they are combined with mathematical expressions or logical functions.

A.2.2.3 Key elements

WCA generally consists of the following steps:

– identification of the relevant system and its components;
– identification of the mathematical or logical function to explain the objective system performance with its parameters describing component performance;
– identification of tolerance limits of system parameters;
– analysis of system performance characteristics for all the combinations of given system parameter tolerance limits;
– verification of the results with the given specifications of the system performance;
– identification of recommended actions to redesign the system configuration;
– follow-up actions to close out recommended actions;
– documentation of analytical processes and final results.

A.2.2.4 Benefits

– The designer can be confident that the system has high reliability for the drift of component characteristics, provided all the analytical results are inside specifications.
– No complex mathematical treatments are needed.
– Analytical results are frequently accurate.

A.2.2.5 Limitations

– All mathematical and logical relationships between parameters are required.
– All the system components are included to obtain reasonable analytical results.
– Analytical results are not optimum values.

A.2.3 Variation simulation modelling

A.2.3.1 Description and purpose

Variation simulation modelling consists of a set of statistical approaches to be used to confirm and determine whether or not the system performance can fall within specifications under all the combinations of given tolerance limits of the system parameters. There are two typical statistical methods: the Moment method and the Monte Carlo method. The former model, designed for the system performance variable, is based on the linear approximation of a function of design parameters in the Taylor series concerning nominal values. The latter model is based on the simulation by statistical methods that each design parameter is randomly selected on a given probability distribution.

A.2.3.2 Application

Variation simulation modelling is generally used for the system composed of several components together with the worst case method mostly during the design and development phase. For example, any designed mechanism, circuit, or network can be considered as the system. The component performance characteristics as well as the design parameters of the system can affect the system performance characteristics. The Monte Carlo simulation is frequently performed during computer aided design (CAD) processes.

A.2.3.3 Key elements

Variation simulation modelling generally consists of the following steps:

a) Common elements
   - identification of the relevant system and its components;
   - identification of the system performance function expressed with all of component performance or design parameters;
   - identification of tolerance limits of system parameters.

b) Moment method
   - establishment of the linear approximation of the system performance function in the Taylor series;
   - identification of the nominal values and variances of the design parameters;
   - identification of the nominal value and variance of system performance calculated on the design parameters.

c) Monte Carlo simulation
   - identification of the probability distribution for each design parameter;
   - identification of random variable generation for design parameters based on the given probability distribution by computer;
   - identification of the probability distribution, its mean and variance of system performance by simulation.

d) Common elements
   - verification of the results with the prescribed specifications of the system performance;
   - identification of recommended actions to redesign the system configuration;
   - follow-up actions to close out recommended actions;
   - documentation of analytical processes and final results.

A.2.3.4 Benefits

a) Moment method:
   - the designer can be confident that the system has specified reliability for the drift of component characteristics if all the analytical results are inside specifications;
   - analytical results provide more precise interval estimation than WCA.

b) Monte Carlo simulation:
   - the designer can be confident that the system has specified reliability for the drift of component characteristics, provided all the analytical results are inside specifications;
   - it is suitable for computerized design;
   - any probability distribution is simulated;
   - simulated results are usually near to optimum;
   - no complex mathematical treatments are needed.

A.2.3.5 Limitations

a) Moment method:
   - mathematical models capable of differentiation are required;
   - all the system components need to be included in order to obtain reasonable analytical results;
   - complex mathematical treatments are needed;
   - the probability distribution is assumed to be the normal distribution.

b) Monte Carlo simulation:
   - mathematical models for simulation are required;
   - all the system components need to be included in order to obtain reasonable analytical results;
   - a large number of replicas of the system are simulated.

A.2.4 Software reliability engineering (SRE)

A.2.4.1 Description and purpose

The purpose of SRE is to predict the reliability of software through statistical methods. The problem is that, in principle, software does not fail, but delivers deterministically correct or erroneous results for a given fixed input. The underlying model therefore does not assume that the software acts randomly, but that the system configuration and the operation profile (e.g. input data) can be viewed as a random environment.

A.2.4.2 Application

SRE can either be applied during testing as a means to decide when to stop testing (assuming that an acceptance criterion has been set) or to predict the reliability in the field. Usually the data are sampled in groups, e.g. as number of failures per cumulated execution time, as it is very hard to get real inter-arrival times for failures.

In most applications it is assumed that software failure can be described as a non-homogeneous Poisson process. This means that software failures occur at statistically independent and exponentially distributed inter-arrival times, but that the failure intensity varies with time. Generally, a decreasing failure intensity is assumed, which means that the models assume that errors, once they are found, are effectively removed, at least without introduction of new bugs. The major objective of SRE is to determine the form of the failure intensity function and to estimate its parameters from observed failure data. Once the failure intensity function has been determined, several reliability measures can be derived such as:

- cumulative number of failures;
- number of remaining failures;
- time to next failure;
- residual test time (until acceptance);
- maximum number of failures (with respect to the lifetime).

Other approaches take into account the software architecture as functional modules and model first their interaction and execution behaviour, e.g. by Markov processes. In a second step, data are sampled and evaluated for the modules.

A.2.4.3 Key elements

– Define the relevant reliability measures and objectives.
– Define the software reliability model to be used.
– Sample failure data.
– Validate the model.
– Predict reliability measures from the data.

A.2.4.4 Benefits

– Software can be included in reliability predictions.
– Objective test end criteria can be defined and controlled.

A.2.4.5 Limitations

– Collection of software reliability data can be difficult. The results are only as good as the data collected.
– There exist a variety of approaches, but no standard has yet been set for the approach or for the failure intensity functions. There is a temptation to select the model to which the data fit best instead of selecting the model a priori.
– The theoretical foundation for the non-homogeneous Poisson process is much weaker than in the case of hardware reliability prediction.

A.2.5 Finite element analysis

A.2.5.1 Description and purpose

Finite element analysis is a computer-based numerical method for analysing the effects of applied loads to physical items. Loads can be mechanical, thermal, electromagnetic, fluid, or combinations of these. Usually the problem addressed is too complex for classical methods.

This technique differs fundamentally from classical methods in terms of its treatment of an item. The infinitesimal differential elements used in calculus, differential and partial differential equations consider the item as a continuum. For finite element analysis, the item is divided into simple interrelated building blocks called elements. Elements are characterized by shape functions. Collectively, they form a geometric model of the item. Elements are interconnected at nodes. Information is passed from element to element only at the level of common nodes. Interpolation is used to assure continuity within elements and across element boundaries. Thus, effects at any point within the item can be expressed in terms of nodal displacements.

A.2.5.2 Application

Finite element analysis is an effective method for predicting behaviour and failure modes in complex structures. It can be used for analysing many different types of problems, including mechanical stress analysis, vibration, fluid flow, heat transfer, electromagnetic fields and others.

A.2.5.3 Key elements (steps)

– Select the most appropriate type of finite elements for modelling the item.
– Divide the item into elements and define element properties.
– Assemble a matrix representation of the interaction among the degrees of freedom of the nodes.
– Define boundary conditions and apply loads.

– Solve the set of algebraic equations for the matrix to calculate nodal displacements.
– Calculate physical parameters of interest, e.g. stress, vibrational modes.

A.2.5.4 Benefits

– Can be used for analysing both elastic and inelastic effects.
– Can be used for performing both static and dynamic analyses.
– Can be used to analyse items with irregular shapes, multiple boundary conditions and loads as well as various materials.
– Can be used to optimize designs.
– Can be used to assess and validate reliability.

A.2.5.5 Limitations

– Requires a high level of specialized technical expertise.
– Easy to misinterpret or misapply results.

A.2.6 Parts derating and selection

A.2.6.1 Description and purpose

Parts are selected, taking into account two criteria, part reliability and part ability to withstand the expected environmental and operational stresses when used in a product. Part selection addresses both, i.e. part required reliability as well as its mechanical and/or electrical rating along with the description of environments in which the parts are to operate without experiencing a failure.

Each component type, whether electronic (active or passive) or mechanical, shall be evaluated to ensure that its temperature rating, construction and other specific attributes (mechanical or other) are adequate for intended environments. This task can be accomplished using the following steps:

a) Evaluate the thermal profile prepared for a product (inside the enclosure). If no such profile has been prepared, discuss with the design team what would be the worst case temperature expected.
b) Review other product environmental requirements (climatic and dynamic).
c) Compare the findings in steps a) and b) to the component specifications to determine whether each component type is capable of meeting thermal and other environments.

Parts should also be selected to ensure their acceptable reliability. Each part has a certain probability of failure that is dependent on part application, part construction and part complexity. The product (assembly) in which this part is supposed to operate has its own reliability requirements. For that reason, the key parts of an assembly or product, i.e. those parts that are essential to the product operation for their specific performance (the “must have” parts) need to be selected in such a way so as to have an acceptable probability of survival.

Derating a part means subjecting it to reduced operational and environmental stresses, the goal being to reduce its failure probability to within period of time required for product proper operation.

When comparing the rated component strength to the expected stress, it is important to allow for a margin, which may be calculated based on the cumulative or fatigue stress and the component strength, or based on other engineering analysis criteria and methods. This margin allows for achievement of the desired part reliability regarding the particular fault modes and the respective causes.

A.2.6.2 Application

Selection of parts for conformance with the expected environments and for reliability shall be applied to any product reliability task. Part derating shall be applied as an integral part of all design efforts, insofar as an improperly derated part may be a cause of product unreliability.

A.2.6.3 Key elements

The key elements of this process are as follows:

– information on part operational and storage environments;
– information on part reliability in the environment for which the product is designed;
– derating guidelines, prepared with a view to product reliability and the best design practices.

A.2.6.4 Benefits

The benefit of the parts selection and derating practices is the achievement of the product's desired reliability.

A.2.6.5 Limitation

The only limitation of this practice is when there is no information on part reliability in any of the available databases or from the part manufacturer. In such a case, limitation extends to the part derating when the derating guidelines involve reliability guidelines. Where derating guidelines are followed, regardless of reliability, limitations may include over-derating.

A.2.7 Pareto analysis

A.2.7.1 Description and purpose

Pareto analysis, based on the Pareto principle developed by Vilfredo Pareto (an Italian economist), is one of the “seven basic quality control tools” (check sheets, Pareto charts, Ishikawa diagrams, flow diagrams, histograms, scatter plots and control charts). These tools, even when developed and broadly used in the field of quality control, may find useful application in the field of dependability engineering. The Pareto principle states that a small subset of problems (the “vital few”) affecting a common outcome tend to occur much more frequently than the remainder (the “useful many”). This principle can also be defined as “20 % of the sources cause 80 % of any problem”.

The purpose of the Pareto analysis is to focus efforts on those problems that have the highest potential for improvement and to help in prioritizing resources where they are most effective.

The Pareto chart is one of the most used improvement tools. It shows the relative importance of problems in a simple, quickly interpreted, visual form. In addition, it helps prevent “shifting the problem” where the “solution” removes some causes but worsens others. It may also allow for the measurement of an impact of a design change upon product performance through the management of variations:

– major cause breakdowns: in this case the “tallest bar” is broken into subclauses in a linked Pareto chart;
– before and after analysis: in this case the new Pareto bars are drawn side-by-side with the original Pareto, showing the effect of a change;
– change the source of data: in this case data is collected on the same problem, but from different sources (systems/equipment, location, customer, etc.) and shown in side-by-side Pareto charts;
– change measurement: in this case the same categories are used, but measured differently (i.e. cost and frequency).

A.2.7.2 Application

Pareto analysis can be used during all phases of the dependability program, from concept and definition, design and development, manufacturing and installation to operation and maintenance.

A.2.7.3 Key elements

To apply Pareto analysis techniques effectively requires the following considerations:

– decide which problem you want to know more about (i.e. failures and related causes);
– choose the causes or problems that will be monitored, compared, and rank ordered (by existing data, brainstorming, expert knowledge);
– choose the most meaningful unit of measurement such as frequency or cost;
– choose the time period for the study;
– assemble the data to be analysed listing the items in order of magnitude, starting with the largest;
– calculate the total of all the items, and the percentage that each item represents of the total;
– draw the bar chart listing the categories on the horizontal line and frequencies (or costs) on the vertical line;
– draw in a cumulative curve, if appropriate;
– label the diagram with appropriate titles, etc.;
– interpret the results.

A.2.7.4 Benefits

– It presents to the user an effective graphic representation of the analysed problem.
– It is a very simple technique and does not require much time and effort.
– It can be used for decision-making in technical as well as non-technical areas.

A.2.7.5 Limitations

– The Pareto chart is only a tool to facilitate the display of data. Investigation into the cause of a problem needs to be conducted by experts using any appropriate technique.
– Experience (and common sense) has to be used; certain customer complaints may deserve more attention than others, depending on who the customer is and what the complaint is.

A.2.8 Cause and effect diagram

A.2.8.1 Description and purpose

The cause and effect diagram, also called the Ishikawa diagram (after its creator, Kaoru Ishikawa of Japan) or the fishbone diagram (due to its shape), provides a pictorial display of a list in which possible causes of problems, or factors needed to ensure success or failure, can be identified and organized.

It is an effective tool that allows one to easily see the relationship between factors when studying processes and situations as well as for planning.

Cause and effect diagrams are typically constructed through brainstorming techniques. As a result, they are often drafted by hand on paper. However, software packages capable of displaying the diagram professionally are available.

1) Definition of the effect
2) Identification of the main causes
3) Identification of secondary causes
4) Identification of the most probable secondary causes

NOTE For step b), the 4 M-method is often used: man, machinery, methods and materials. Other main causes can also be used, e.g. steps of a process.

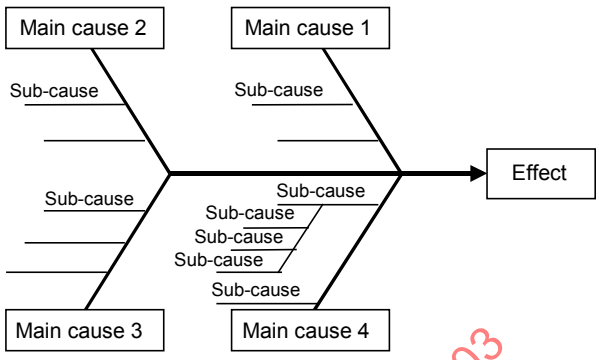


Figure A.15 – Cause and effect diagram

A.2.8.2 Application

The cause-effect diagram is used for preliminary analyses during the design phase and analysis of effects encountering during operation.

A.2.8.3 Key elements

– The effects have to be understandable to everyone.
– The causes stated have to be relevant to the effect.
– An appropriate choice of secondary causes helps to balance the tree structure.
– As real causes have to be supported by data and facts, this information has to be available.
– Substructures which become too complex or remain too simple could be an indication that the structure can be improved to allow for better evaluation.

A.2.8.4 Benefits

– Encourages and supports the work with interdisciplinary teams.
– Provides a visual expression of causes and their clustering.
– Results can be used as input to FMEA or fault tree analysis.

A.2.8.5 Limitations

– No quantitative analyses.
– Choice of correct causes and secondary causes depends on experience of the team.
– Multiple consequences are not covered.

A.2.9 Failure reporting analysis and corrective action (FRACAS)

A.2.9.1 Description and purpose

FRACAS is a closed-loop system for identifying, assessing and correcting failure related problems in a timely manner. Failures occurring during testing and evaluation are documented. Data are collected at multiple levels. The system is used to track, analyse and subsequently identify part problems, design errors, workmanship defects and process deficiencies requiring corrective action. Development of corrective actions follows determination of the root cause of failure. The effectiveness of corrective actions is verified before implementation.

A.2.9.2 Application

FRACAS should be in place as soon as hardware and software become available. All personnel involved in testing and evaluation are responsible for documenting failures. Failures are verified and localized to the extent possible.

A review team analyses the data to determine the significance of the problems, to determine which problems require corrective action and to assure that they are properly resolved. All disciplines likely to be affected by the problems are represented on the team.

Failure analyses are performed to levels necessary to formulate corrective actions to eliminate problems. Verification of the effectiveness of the corrective actions includes determination by the team that recurrence of failures is prevented.

A.2.9.3 Key elements

– A reporting format tailored to the system under development and the development process.
– A database suitable for documenting all activities related to the analysis and resolution of problems.
– A multidisciplinary review team.
– A mechanism for tracking the resolution of problems.

A.2.9.4 Benefits

– Can use data collected under widely different operational and environmental conditions.
– Can be implemented for design, manufacturing and maintenance.
– Can be an important contributor to reliability growth.
– Can use data from past projects and provide data for future projects.

A.2.9.5 Limitations

– Only prevents the recurrence of problems.
– Dependent upon those involved in testing, evaluation and service to report failures.
– Often impractical to combine data for numerical estimates.

Bibliography

This bibliography serves as a starting point for further reading. The goal is to give only one representative source.

IEC 60300-2:1995, *Dependability management – Part 2: Dependability programme elements and tasks*

Failure rate prediction

BAJENESCU, T.I., BAZU, M.I., *Reliability of Electronic Components*, Springer, 1999

FTA

ROBERTS, *et al.* (1981) "*Fault Tree Handbook*", US Nuclear Regulatory Commission, Washington, D.C., USA, 1981

ETA

ANG, A. H-S. TANG, W.H., *Probability Concepts in Engineering Planning and Design; Volume II Decision, Risk, and Reliability*, 1990

RBD

SAE JA1000-1 *Reliability Program Standard Implementation Guide*; Issued 1999-03

Markov analysis

STEWART, W.J., *Introduction to the Numerical Solution of Markov Chains*, Princeton University Press, 1994

Petri net analysis

SCHNEEWEISS, W., *Petri Nets for Reliability Modeling*, LiLoLe, Hagen, 1999

FMEA

SAE ARP5580 "*Failure mode, effects and criticality analysis*"

SAE J1739 *Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) Reference Manual*

HAZOP

REDMILL, F., CHUDLEIGH, M., CATMUR, J., *HAZOP and Software HAZOP*, Wiley,1999

Human reliability analysis

Dhillon, B.S., *Human Reliability with Human Factors*, Pergamon Press, 1988

Stress-strength analysis

Shu-Ho Dai, Ming-O Wang, *Reliability Analysis in Engineering Applications*, van Nostrand Reinhold, New York, 1992

Truth table

VILLEMEUR, A., *Reliability, Availability, Maintainability and Safety Assessment*, vol. 1 and vol. 2, John Wiley & Sons, 1992

Statistical reliability methods

MEEKER, W.Q., ESCOBAR, L.A., *Statistical methods for reliability data*, John Wiley, 1998

Sneak circuit analysis

GODOY, S.G., ENGELS, G.J., *Sneak Analysis and Software Sneak Analysis*, J. Aircraft Vol. 15, No. 8, 1978

Worst-case analysis

IRESON, W.G., COOMBS, C.F.Jr., MOSS, R.Y., *Handbook of Reliability Engineering and Management*, McGraw-Hill 1996

Variation simulation modelling

LAW, A.M., KELTON, W.D., *Simulation modelling and analysis*, McGraw-Hill, 1991

Software reliability engineering

LYU, M.R. (Ed.): *Handbook of Software Reliability Engineering, IEEE Computer Society Press, 1995*

Finite element analysis

ADAMS, A., ASKENAZI, M.V., *Building Better Products With Finite Element Analysis*, Thomson Learning, 1998

Parts derating and selection

FUQUA, N.B., *Reliability Engineering for Electronic design*, Dekker, 1986

Pareto analysis

SAE JA-1, *Reliability Program Standard Implementation Guide*, Warrendale, PA, 1999

Cause and effect diagrams

KUNE, H., *Statistical Methods for Quality Improvement*, AOTS, 1985

FRACAS

MIL-HDBK-2155, *Failure Reporting, Analysis and Corrective Action System (FRACAS),* 1995

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique

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 60300-3-1 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette seconde édition annule et remplace la première édition, publiée en 1991, dont elle constitue une révision technique. Les lignes directrices concernant le choix de techniques d'analyse et le nombre des techniques couvertes ont notamment été étendues.

La présente version bilingue (2013-03) correspond à la version anglaise monolingue publiée en 2003-01.

Le texte anglais de cette norme est issu des documents 56/825/FDIS et 56/840/RVD.

Le rapport de vote 56/840/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2007. 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

Les techniques d'analyse décrites dans la présente partie de la CEI 60300 servent à prévoir, examiner et améliorer la fiabilité, la disponibilité et la maintenabilité d'une entité.

Ces analyses sont effectuées pendant les phases de faisabilité et de définition, de conception et de développement, d'exploitation et de maintenance, à des niveaux différents et avec plus ou moins de détails afin d'évaluer, déterminer et améliorer les mesures de sûreté de fonctionnement d'une entité. Les analyses permettent également de comparer les résultats de l'analyse avec les exigences prescrites.

Elles sont également appliquées dans la planification de la logistique et de la maintenance pour estimer la fréquence de maintenance et de remplacement des pièces. Ces estimations déterminent souvent les principaux éléments du coût du cycle de vie, et il convient de les appliquer avec attention dans les études de ce coût et les études comparatives.

Afin de fournir des résultats significatifs, il convient que l'analyse prenne en compte tous les éléments potentiels contribuant à la sûreté de fonctionnement d'un système tels que les matériels, les logiciels, les facteurs humains et les aspects liés à l'organisation.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique

1 Domaine d'application

La présente partie de la CEI 60300 donne une vue générale des techniques d'analyse de la sûreté de fonctionnement communément employées. Elle décrit les méthodologies habituelles, les avantages et les inconvénients, les données d'entrée et les autres conditions concernant l'utilisation de techniques différentes.

La présente norme constitue une introduction aux méthodologies sélectionnées et est destinée à fournir les informations nécessaires permettant de choisir les méthodes d'analyse les plus appropriées.

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 (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-2:1993, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 2: Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

CEI 60300-3-4:1996, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 4: Spécification d'exigences de sûreté de fonctionnement*

CEI 60300-3-5:2001, *Gestion de la sûreté de fonctionnement – Partie 3-5: Guide d'application – Conditions des essais de fiabilité et principes des essais statistiques*

CEI 60300-3-10:2001, *Gestion de la sûreté de fonctionnement – Partie 3-10: Guide d'application – Maintenabilité*

CEI 60706-1:1982, *Guide de maintenabilité du matériel – Partie 1: Sections Un, Deux et Trois – Introduction, exigences et programme de maintenabilité*

CEI 60706-2:1990, *Guide de maintenabilité du matériel – Partie 2: Section Cinq – Études de maintenabilité pendant la phase de conception*

CEI 60812:1985, *Techniques d'analyse de la fiabilité des systèmes – Procédures d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 61078:1991, *Techniques d'analyse de la sûreté de fonctionnement – Méthode du bloc-diagramme de fiabilité*

CEI 61165:1995, *Application des techniques de Markov*

CEI 61709:1996, *Composants électroniques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles d'influence des contraintes pour la conversion*

CEI 61882:2001, *Études de danger et d'exploitabilité (études HAZOP) – Guide d'application*

ISO 9000:2000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

3 Définitions

Pour les besoins de la présente partie de la CEI 60300, les définitions données dans la CEI 60050(191), dont certaines sont reproduites ci-dessous, ainsi que les définitions suivantes, s'appliquent.

3.1
entité, dispositif, individu
tout élément, composant, sous-système, unité fonctionnelle, équipement ou système que l'on peut considérer individuellement

NOTE Une entité peut être constituée de matériel, de logiciel ou des deux à la fois, et peut aussi, dans certains cas, comprendre le personnel.

[VEI 191-01-01]

3.2
système
ensemble d'éléments corrélés ou interactifs

[ISO 9000,2000]

NOTE 1 Dans le contexte de la sûreté de fonctionnement, un système disposera

a) d'un objet défini exprimé en termes de fonctions prévues, et

b) de conditions spécifiées de fonctionnement/utilisation.

NOTE 2 Le concept d'un système est hiérarchique.

3.3
composant
entité du plus bas niveau considéré dans l'analyse

3.4
allocation
procédure mise en oeuvre pendant la conception d'une entité en vue de répartir les exigences imposées aux caractéristiques relatives à cette entité entre ses sous-entités, conformément à des critères donnés

3.5
défaillance
cessation de l'aptitude d'une entité à accomplir une fonction requise

NOTE 1 Après défaillance d'une entité, cette entité est en état de panne.

NOTE 2 Une défaillance est un passage d'un état à un autre, par opposition à une panne, qui est un état.

[VEI 191-04-01]

3.6
panne,
état d'une entité inapte à accomplir une fonction requise, à l'exclusion de l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou due à un manque de moyens extérieurs

NOTE Une panne est souvent la conséquence d'une défaillance de l'entité elle-même, mais elle peut exister sans défaillance préalable.

[VEI 191-05-01]

4 Procédure de base de l'analyse de la sûreté de fonctionnement

4.1 Procédure générale

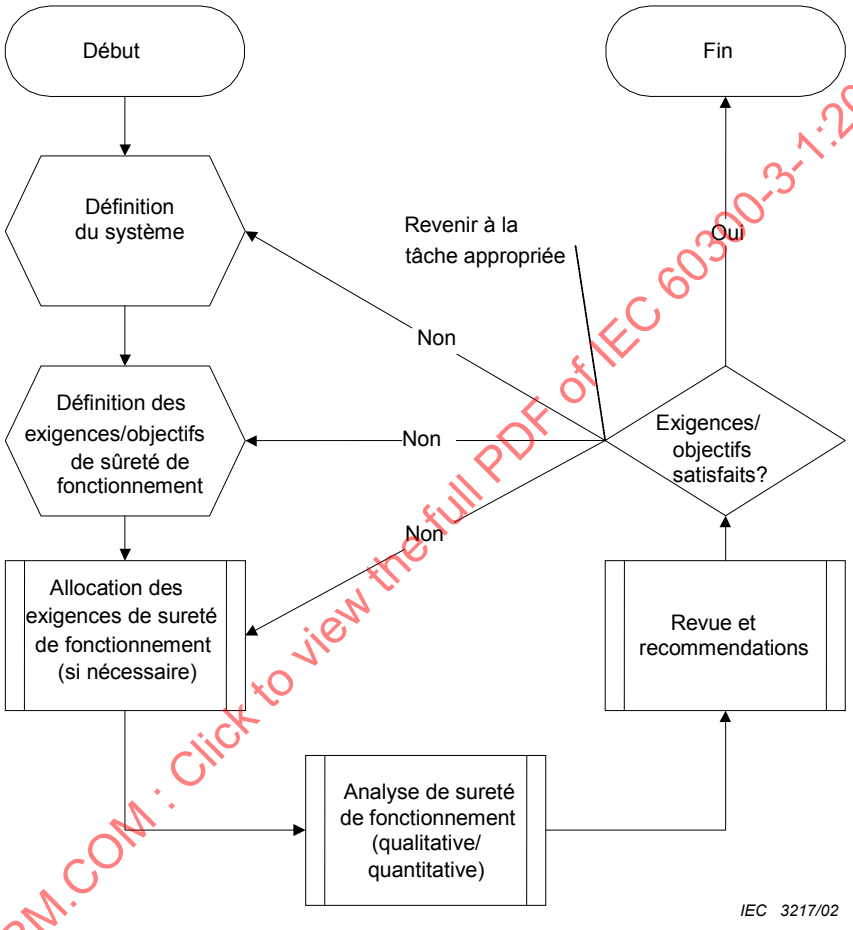


Figure 1 – Procédure générale d'analyse de la sûreté de fonctionnement

Une procédure générale d'analyse de la sûreté de fonctionnement comprend les tâches suivantes (le cas échéant):

a) Définition du système

Définir le système à analyser, ses modes de fonctionnement, les relations fonctionnelles avec son environnement, y compris les interfaces ou les processus. La définition du système constitue généralement un élément d'entrée (intrant) du processus d'ingénierie de ce même système.

b) Définition des exigences/objectifs de la sûreté de fonctionnement

Établir la liste de toutes les exigences ou de tous les objectifs, et de toutes les caractéristiques et fonctionnalités concernant la fiabilité et la disponibilité du système, ainsi que les conditions environnementales et opérationnelles, et les exigences concernant la maintenance. Définir la défaillance du système, les critères et les conditions de défaillance sur la base de ses spécifications fonctionnelles, ainsi que de la durée et de

l'environnement d'exploitation prévus (profil et temps de mission). Il convient d'utiliser la CEI 60300-3-4 comme ligne directrice.

c) Allocation des exigences concernant la sûreté de fonctionnement

Affecter les exigences ou les objectifs concernant la sûreté de fonctionnement du système aux différents sous-systèmes dans la phase de conception initiale si nécessaire.

d) Analyse de la sûreté de fonctionnement

Analyser le système habituellement sur la base des techniques de sûreté de fonctionnement et des données de performance appropriées.

1) Analyse qualitative

- Analyser la structure fonctionnelle du système
- Déterminer les modes de panne du système et de ses composants, les mécanismes de défaillance, ainsi que les causes, effets et conséquences des défaillances.
- Déterminer le mécanisme de détérioration susceptible d'engendrer des défaillances.
- Analyser les chemins défaillance/panne.
- Analyser la maintenabilité compte tenu du temps, de la méthode de localisation et de réparation du problème.
- S'assurer de l'adéquation des diagnostics fournis pour détecter les pannes.
- Analyser toute possibilité d'évitement des pannes.
- Déterminer les stratégies de maintenance et de réparation potentielles, etc.

2) Analyse quantitative

- Développer les modèles de fiabilité et/ou disponibilité.
- Définir les données de référence numériques à utiliser.
- Effectuer des évaluations de sûreté de fonctionnement numériques.
- Réaliser des analyses de criticité et de sensibilité des composants si nécessaire.

e) Revue et recommandations

Analyser si les exigences/objectifs de sûreté de fonctionnement sont satisfaites et si des conceptions alternatives peuvent améliorer en terme de rentabilité la sûreté de fonctionnement. Les activités peuvent inclure les tâches suivantes (selon le cas):

- Évaluer l'amélioration de la sûreté de fonctionnement du système à la suite de l'amélioration de la conception et de la fabrication (par exemple, redondance, réduction des contraintes, amélioration des stratégies de maintenance, systèmes d'essai, processus technologiques et système de contrôle de qualité).

  NOTE 1 Les mesures de performances intrinsèques de la sûreté de fonctionnement peuvent être améliorées par la seule conception. Lorsqu'un mauvais procédé de fabrication génère de faibles valeurs de mesure, il est possible, d'un point de vue opérationnel, d'améliorer les mesures de performances de sûreté de fonctionnement observées par l'amélioration du procédé de fabrication.

- Revoir la conception du système, et déterminer les faiblesses et les modes de pannes et composants critiques.
- Tenir compte des problèmes d'interface système, des caractéristiques et mécanismes de sûreté intégrée, etc.
- Développer d'autres méthodes d'amélioration de la sûreté de fonctionnement, par exemple, redondance, contrôle des performances, détection des pannes, techniques de reconfiguration du système, procédures de maintenance, capacité de remplacement des composants et procédures de réparation.
- Réaliser des études de rentabilité qui permettent d'évaluer le coût et la complexité des conceptions alternatives.
- Évaluer l'influence de la capacité du procédé de fabrication.
- Évaluer les résultats et les comparer avec les exigences.

NOTE 2 La procédure générale résume, d'un point de vue technique, les éléments spécifiques de programme de sûreté de fonctionnement définis dans la CEI 60300-2, qui s'appliquent pour l'analyse et les spécifications de ladite sûreté, l'analyse de l'environnement d'utilisation, l'ingénierie de fiabilité et de maintenabilité, les facteurs humains, la modélisation et la simulation de la fiabilité, l'analyse de conception et l'évaluation du produit, l'influence des causes et des effets et l'analyse du risque, la prévision et l'analyse de rentabilité.

4.2 Méthodes d'analyse de la sûreté de fonctionnement

Les méthodes définies dans la présente norme relèvent de deux catégories principales:

– les méthodes utilisées principalement pour l'analyse de la sûreté de fonctionnement;

– les méthodes d'ingénierie générale qui viennent à l'appui de l'analyse de la sûreté de fonctionnement ou qui apportent une valeur ajoutée à la conception dédiée à ladite sûreté.

L'applicabilité des méthodes d'analyse de la sûreté de fonctionnement dans le cadre des tâches générales de cette analyse propres à la procédure d'analyse générale est indiquée dans le Tableau 1. Le Tableau 2 spécifie des caractéristiques plus détaillées. Les méthodes sont expliquées de manière succincte à l'Annexe A.

Tableau 1 – Utilisation des méthodes applicables dans le cadre des tâches générales de l'analyse de la sûreté de fonctionnement

Méthode d'analyse	Allocation des exigences/objectifs concernant la sûreté de fonctionnement	Analyse qualitative	Analyse quantitative	Revue et recommandations	Annexe
Prévision du taux de défaillance	Applicable pour des systèmes en série sans redondance	Possible pour une analyse de la stratégie de maintenance	Calcul des taux de défaillance et du MTTF pour les composants et matériels électroniques	Prise en charge	A.1.1
Analyse par arbre de panne	Applicable, si le comportement du système ne dépend pas dans une large mesure du temps ou de la séquence	Combinaisons de pannes	Calcul de la fiabilité et de la disponibilité du système et contributions relatives des sous-systèmes à l'indisponibilité du système	Applicable	A.1.2
Analyse par arbre d'événement	Possible	Séquences de défaillances	Calcul des taux de défaillance du système	Applicable	A.1.3
Analyse par bloc-diagramme de fiabilité	Applicable, pour les systèmes avec lesquels on peut supposer l'existence de blocs indépendants	Parcours de réussite	Calcul de la fiabilité et de la disponibilité du système	Applicable	A.1.4
Analyse de Markov	Applicable	Séquences de défaillances	Calcul de la fiabilité et de la disponibilité du système	Applicable	A.1.5
Analyse par réseau de Pétri	Applicable	Séquences de défaillances	Décrire le système pour une analyse de Markov	Applicable	A.1.6
Analyse des modes de défaillance, de leurs effets et de leur criticité, AMDEC	Applicable, pour les systèmes avec lesquels une défaillance unique indépendante prédomine	Effets des défaillances	Calcul des taux de défaillance (et de la criticité) du système	Applicable	A.1.7
Études HAZOP	Prise en charge	Causes et conséquences des écarts	Non applicable	Prise en charge	A.1.8

Méthode d'analyse	Allocation des exigences/objectifs concernant la sûreté de fonctionnement	Analyse qualitative	Analyse quantitative	Revue et recommandations	Annexe
Analyse de fiabilité du personnel	Prise en charge	Influence des facteurs humains sur l'exploitation du système	Calcul des probabilités d'erreur pour les tâches du personnel	Prise en charge	A.1.9
Analyse contrainte-résistance	Non applicable	Utilisable comme moyen d'évitement des pannes	Calcul de la fiabilité pour les composants (électro)mécaniques	Prise en charge	A.1.10
Table de vérité (analyse des fonctions de structure)	Non applicable	Possible	Calcul de la fiabilité et de la disponibilité du système	Prise en charge	A.1.11
Méthodes de fiabilité statistique	Possible	Influence des pannes	Estimation quantitative de la fiabilité avec des incertitudes	Prise en charge	A.1.12

NOTE Le libellé particulier du tableau est le suivant:

"Applicable" signifie que la méthode est généralement applicable et recommandée pour la tâche concernée (le cas échéant avec les limites mentionnées).

"Possible" signifie que la méthode peut être utilisée pour cette tâche mais comporte certains inconvénients par comparaison avec d'autres méthodes.

"Prise en charge" signifie que la méthode est généralement applicable pour une certaine partie de la tâche, mais non comme une méthode autonome pour la tâche complète.

"Non applicable" signifie que la méthode ne peut pas être utilisée pour cette tâche.

Les méthodes d'ingénierie de prise en charge ou générales comportent entre autres les méthodes suivantes (la liste n'est pas nécessairement exhaustive):

– études de maintenabilité (couvertes par la CEI 60300-3-10 en général et la CEI 60706-2 en particulier);
– analyse de circuits insidieux (A.2.1);
– analyse du cas le plus défavorable (A.2.2);
– modélisation par simulation des variations (A.2.3);
– ingénierie de fiabilité logicielle (A.2.4);
– analyse par éléments finis (A.2.5);
– déclassement et sélection des pièces (A.2.6);
– analyse de Pareto (A.2.7);
– diagrammes cause-effet (A.2.8);
– système de notification des défaillances et d'actions correctives (A.2.9).

Il convient également de noter que les méthodes sont dénommées et comprises au sens des normes CEI applicables (lorsqu'elles existent). Les méthodes suivantes n'ont pas été incluses comme méthodes distinctes dans la mesure où elles sont issues ou étroitement associées aux méthodes principales:

– l'analyse cause/conséquence est une combinaison des AAE et AAP;
– l'AAP dynamique est une extension de l'AAP, où certains événements sont exprimés par des sous-modèles de Markov;
– l'analyse des défaillances de fonctionnement est un type particulier de l'AMDE;
– les diagrammes de décision binaire sont utilisés principalement comme représentation efficace des arbres de panne.

4.3 Allocations de la sûreté de fonctionnement

Définir les exigences concernant la sûreté de fonctionnement des sous-systèmes constitue une partie essentielle du travail de conception du système. L'objectif de cette tâche consiste à déterminer l'architecture système la plus efficace permettant de satisfaire aux exigences de sûreté de fonctionnement (et ainsi de contribuer à l'étude de faisabilité). Dans la mesure où la sûreté de fonctionnement est le terme collectif qui désigne la fiabilité, la disponibilité et la maintenabilité, une allocation s'impose pour chacune de ces caractéristiques. Les techniques d'allocation applicables à l'ensemble de ces trois caractéristiques étant toutefois similaires, le terme collectif sûreté de fonctionnement est utilisé dans cette instance.

La première étape consiste à allouer les exigences de sûreté de fonctionnement du système global aux sous-systèmes, selon la complexité de ces sous-systèmes sur la base de l'expérience acquise avec des sous-systèmes comparables. Lorsque la conception initiale ne permet pas de satisfaire aux exigences, l'allocation et/ou la conception doivent être répétées. L'allocation est également réalisée sur la base d'éléments pris en compte, tels que la complexité, la criticité, le profil d'exploitation et les conditions environnementales.

Étant donné que l'allocation de la sûreté de fonctionnement est normalement requise à une phase préliminaire avec des informations peu nombreuses ou en l'absence d'informations, il convient d'actualiser cette allocation de façon périodique.

L'allocation, parfois appelée répartition, de la sûreté de fonctionnement du système aux sous-systèmes et aux niveaux d'assemblage est nécessaire dès le début de la phase de définition du produit afin:

– de vérifier la faisabilité des exigences de sûreté de fonctionnement pour le système;
– d'établir des exigences réalistes concernant le calcul de la sûreté de fonctionnement à des niveaux inférieurs;
– d'établir des exigences de sûreté de fonctionnement claires et vérifiables applicables aux sous-contractants.

Les étapes suivantes sont nécessaires pour l'allocation de la sûreté de fonctionnement:

– Analyser le système et identifier les domaines où la conception est connue et où les informations concernant les valeurs des caractéristiques de sûreté de fonctionnement sont disponibles, ou peuvent être évaluées immédiatement.
– Attribuer les facteurs de pondération appropriés et déterminer leur contribution aux exigences concernant la sûreté de fonctionnement du système de haut niveau. La différence constitue la partie des exigences de sûreté de fonctionnement qui peut être allouée aux autres domaines.

L'allocation de la sûreté de fonctionnement présente les avantages suivants:

– Elle prévoit une méthode de développement du produit destinée à faire évoluer et à comprendre les relations des objectifs de la sûreté de fonctionnement entre le système et ses composants (par exemple, sous-systèmes, matériel, composants).
– Elle considère la sûreté de fonctionnement comme équivalant à d'autres paramètres de conception tels que les caractéristiques de coût et de performances.
– L'allocation prévoit des objectifs spécifiques de sûreté de fonctionnement à l'intention des fournisseurs que ces derniers doivent atteindre dans le cadre de leurs livraisons, ce qui aboutit pour sa part à des procédures de conception et d'approvisionnement améliorées.
– L'allocation peut générer une sûreté de fonctionnement optimale du système dans la mesure où elle tient compte de facteurs tels que la complexité, la criticité et l'influence de l'environnement d'exploitation.

Par ailleurs, il convient de noter certaines limites:

– On suppose souvent que les entités d'un système sont indépendantes, c'est-à-dire que la défaillance d'une entité n'affecte pas les autres entités. Cette restriction limite les avantages que procure la méthode dans la mesure où cette hypothèse est souvent non valide.

– L'allocation de systèmes redondants est plus complexe. Dans ces cas, il est approprié d'employer une méthode itérative afin de vérifier si les objectifs de sûreté de fonctionnement peuvent être atteints pour le système, par exemple, la méthode de l'arbre de panne.

4.4 Analyse de la sûreté de fonctionnement

4.4.1 Catégories des méthodes

Les méthodes d'analyse de la sûreté de fonctionnement, expliquées brièvement à l'Annexe A, peuvent être classées selon les catégories suivantes, concernant leur objectif principal:

a) méthodes destinées à éviter les pannes, par exemple,
   1) déclassement et sélection des pièces;
   2) analyse de résistance aux contraintes;

b) méthodes d'analyse architecturale et d'évaluation de la sûreté de fonctionnement (allocation), par exemple,
   1) méthode ascendante (qui traite principalement des effets des pannes uniques),
      – analyse par arbre d'événement (AAE),
      – analyse des modes de défaillance et de leurs effets (AMDE),
      – études de danger et d'exploitabilité (HAZOP),
   2) méthode descendante (capable de tenir compte des effets nés de la combinaison des pannes)
      – analyse par arbre de panne (AAP),
      – analyse de Markov,
      – analyse par réseau de Pétri,
      – table de vérité (analyse des fonctions de structure),
      – diagrammes de fiabilité (BDF),

c) méthodes d'estimation des mesures dédiées aux événements de base, par exemple,
   – prévision du taux de défaillance,
   – analyse de fiabilité du personnel (HRA),
   – méthodes de fiabilité statistique,
   – ingénierie de fiabilité logicielle (SRE).

Une autre différenciation consiste à déterminer si ces méthodes sont accompagnées de séquences d'événements ou de propriétés dépendantes du temps. La prise en compte de cette différenciation génère les résultats de catégorisation exhaustifs suivants:

Séquences dépendantes	Analyse par arbre d'événement	Markov, Pétri, table de vérité
Séquences indépendantes	AMDE, HAZOP	AAP, BDF
	Ascendante (panne unique)	**Descendante (pannes multiples)**

Ces méthodes d'analyse permettent d'évaluer les caractéristiques qualitatives, ainsi que d'estimer les caractéristiques quantitatives afin de prévoir le comportement opérationnel à

long terme. Il convient de noter que la validité de tout résultat dépend clairement de la précision et de l'exactitude des données d'entrée pour les événements de base.

Cependant, aucune méthode d'analyse simple de la sûreté de fonctionnement n'est suffisamment complète et souple pour traiter de toutes les complexités de modélisation potentielles nécessaires pour évaluer les caractéristiques des systèmes réels (matériels et logiciels, structures fonctionnelles complexes, technologies diverses, structures réparables et pouvant faire l'objet d'une maintenance, etc.). Il peut s'avérer nécessaire de prendre en considération plusieurs méthodes d'analyse complémentaires afin d'assurer le traitement approprié de systèmes complexes ou multifonctions.

Dans la pratique, une approche composite, avec une analyse descendante et une analyse ascendante complémentaires, s'est révélée très efficace, notamment en vue d'assurer l'exhaustivité de l'analyse.

4.4.2 Méthodes ascendantes

Le point de départ de toute méthode ascendante consiste à identifier les modes de défaillance au niveau des composants. Pour chaque mode de défaillance, l'effet correspondant sur la performance est déduit pour le niveau de système approprié. Cette méthode "ascendante" permet d'identifier tous les modes de défaillance simple de manière rigoureuse, dans la mesure où elle peut se fier aux listes de pièces ou à d'autres listes de contrôle. Dans les premières phases de développement, l'analyse peut être de nature qualitative et traiter des défaillances fonctionnelles. Ultérieurement, une analyse quantitative peut être effectuée du fait de la mise à disposition des détails de conception des composants.

4.4.3 Méthodes descendantes

Il convient tout d'abord de définir l'événement indésirable ou de réussite de plus haut niveau du système (l'événement de tête). Les causes contributives à cet événement à tous les niveaux sont ensuite définies et analysées.

Le point de départ de l'approche descendante consiste à passer du niveau d'intérêt maximal, à savoir le niveau du système ou du sous-système, à des niveaux successivement inférieurs, afin d'identifier les fonctionnements indésirables du système.

L'analyse est effectuée au niveau du système inférieur suivant afin d'identifier toute défaillance et le mode qui lui est associé, qui peut générer l'effet de défaillance identifié à l'origine. L'analyse est répétée, pour chacune de ces défaillances de second niveau, par un retraçage le long des branches fonctionnelles et les relations avec le niveau inférieur suivant. Ce processus se poursuit tant que le niveau inférieur est souhaité.

L'approche descendante est utilisée pour évaluer les défaillances multiples, y compris les défaillances liées aux séquences, l'existence de pannes dues à une cause commune, ou dans le cas d'un système complexe pour lequel il est plus pratique de commencer l'étude par l'identification de ses défaillances.

4.5 Analyse et examen de la maintenance et des réparations

Le fonctionnement d'un système réparable est fortement influencé par la maintenabilité de ce dernier, ainsi que par les stratégies choisies en matière de réparation ou de maintenance. La mesure des performances de disponibilité représente la méthode d'évaluation appropriée de l'influence de la maintenance et de la réparation sur la sûreté de fonctionnement du système lorsque la garantie d'un fonctionnement à long terme constitue l'exigence critique. La fiabilité est la mesure de performance appropriée lorsque la garantie d'un fonctionnement continu constitue l'exigence critique.

On ne peut normalement réparer un système pendant son fonctionnement, sans l'empêcher de remplir sa fonction, que si une structure redondante du système a été prévue avec des

composants redondants accessibles. Dans ce cas, une réparation ou un remplacement augmente la fiabilité et la disponibilité du système.

Il est habituellement nécessaire d'effectuer une analyse séparée pour évaluer les aspects de réparation et de maintenance d'un système (voir CEI 60706-1, CEI 60706-2 et CEI 60300-3-10).

5 Choix de la méthode d'analyse appropriée

Le choix des méthodes à mettre en oeuvre dans un programme de sûreté de fonctionnement constitue un processus extrêmement individualisé, à un point tel qu'il n'est pas possible de proposer, dans un cadre général, le choix d'une ou de plusieurs méthodes spécifiques. Il convient que le choix de méthodes appropriées résulte de l'effort commun de spécialistes issus du secteur de la sûreté de fonctionnement et de l'ingénierie système. Il convient que ce choix intervienne rapidement dans le développement du programme et fasse l'objet d'une revue quant à son applicabilité.

Toutefois, le choix des méthodes peut être facilité, en utilisant les critères suivants:

a) Complexité du système: les systèmes complexes, par exemple impliquant des caractéristiques de redondance ou de diversité, exigent habituellement un niveau d'analyse plus approfondi que les systèmes plus simples.

b) Nouveauté du système: une conception de système totalement nouvelle peut nécessiter un niveau d'analyse plus approfondi qu'une conception parfaitement éprouvée.

c) Analyse qualitative par rapport à analyse quantitative: une analyse quantitative est-elle nécessaire?

d) Panne unique par rapport à pannes multiples: les effets générés par la combinaison des pannes sont-ils pertinents ou peut-on ne pas en tenir compte?

e) Comportement dépendant du temps ou de la séquence: la séquence d'événements joue-t-elle un rôle dans l'analyse (par exemple, le système échoue uniquement si l'événement A est précédé de l'événement B, et non l'inverse) ou le comportement effectif du système dépend-il du temps (par exemple, modes de fonctionnement dégradés après défaillance, missions progressives)?

f) Peut être utilisé pour des événements dépendants: les caractéristiques de défaillance ou de réparation d'une entité individuelle dépendent-elles de l'état du système?

g) Analyse ascendante par rapport à analyse descendante: les méthodes ascendantes peuvent habituellement être appliquées de manière plus directe, tandis que les méthodes descendantes nécessitent une réflexion et une créativité plus développées, et peuvent par conséquent être plus sujettes à des erreurs.

h) Allocation des exigences de fiabilité: la méthode doit-elle être capable de réaliser une allocation quantitative des exigences de fiabilité?

i) Maîtrise requise: quel est le niveau de formation ou d'expérience nécessaire pour appliquer la méthode de manière significative et correcte?

j) Acceptation et communité: la méthode est-elle communément acceptée, par exemple, par un organisme de réglementation ou un client?

k) Nécessité d'un support d'outils: la méthode nécessite-t-elle un support d'outils (informatique) ou peut-elle être également appliquée manuellement?

l) Contrôle de vraisemblance: une inspection manuelle de la vraisemblance des résultats est-elle facilement réalisable? Dans le cas contraire, les outils disponibles sont-ils validés?

m) Disponibilité des outils: les outils sont-ils disponibles en interne ou dans le commerce? Ces outils disposent-ils d'une interface commune avec d'autres outils d'analyse permettant une réutilisation ou une "exportation" des résultats?

n) Normalisation: existe-t-il une norme qui décrit les caractéristiques de la méthode et la présentation des résultats (par exemple, des symboles)?

Le Tableau 2 donne une vue d'ensemble des diverses méthodes d'analyse de la sûreté de fonctionnement, ainsi que de leurs caractéristiques et fonctionnalités. L'analyse complète d'un système peut nécessiter l'emploi de plus d’une méthode.

Tableau 2 – Caractéristiques des méthodes d'analyse de la sûreté de fonctionnement choisies

Méthode	Convient à des systèmes complexes	Convient à des conceptions de système nouvelles	Analyse quantitative	Convient à une combinaison des pannes	Permet de traiter la dépendance aux séquences	Peut être utilisée pour les événements dépendants	Méthode ascendante ou descendante	Convient à l'allocation de sûreté de fonctionnement	Maîtrise requise (de niveau faible à élevé)	Acceptation et communité	Nécessité d'un soutien assisté	Contrôles de vraisemblance	Disponibilité des outils	Norme CEI
Prévision du taux de défaillance	Non	Oui	Oui	Non	Non	Non	BU	Oui	Faible	Élevé	Moy.	Oui	Élevé	61709
Analyse par arbre de panne (AAP)	Oui	Oui	Oui	Oui	Non	Non	TD	Oui	Moy	Élevé	Moy.	Oui	Élevé	61025
Analyse par arbre d'événement (AAE)	NR	NR	Oui	NR	Oui	Oui	BU	NR	Élevé	Moy.	Moy.	Oui	Moy.	
Analyse par bloc-diagramme de fiabilité (BDF)	NR	NR	Oui	Oui	Non	Non	TD	Oui	Faible	Moy.	Moy.	Oui	Moy.	61078
Analyse de Markov	Oui	Oui	Oui	Oui	Oui	Oui	TD	Oui	Élevé	Moy.	Élevé	Non	Moy.	61165
Analyse par réseau de Pétri	Oui	Oui	Oui	Oui	Oui	Oui	TD	Oui	Élevé	Faible	Élevé	Non	Faible	
Analyse des modes de défaillance et de leurs effets (AMDE)	NR	NR	Oui	Non	Non	Non	BU	NR	Faible	Élevé	Faible	Oui	Élevé	60812
Études HAZOP	Oui	Oui	Non	Non	Non	Non	BU	Non	Faible	Moy	Faible	Oui	Moy.	61882
Analyse de fiabilité du personnel	Oui	Oui	Oui	Oui	Oui	Oui	BU	Non	Élevé	Élevé	Moy.	Oui	Moy.	
Analyse contrainte-résistance	NA	NA	Oui	NA	NA	Non	NA	Non	Élevé	Moy	Élevé	Oui	Moy.	
Table de vérité	Non	Oui	Oui	Oui	Non	Non	NA	Oui	Élevé	Moy	Élevé	Non	Faible	
Méthodes statistiques de fiabilité	Oui	Oui	Oui	Oui	Oui	Oui	NA	NR	Élevé	Moy	Élevé	Moy.	Faible	60300-3-5

NR	Peut être utilisée pour des systèmes simples. Non recommandée comme méthode autonome, à utiliser avec d'autres méthodes.
TD *(Top/Down)*	Méthode descendante.
BU *(Bottom/Up)*	Méthode ascendante.
Avg	Moyenne.
NA	Le critère n'est pas applicable eu égard à la présente méthode.

Annexe A
(informative)

Description succincte des techniques d'analyse

A.1 Techniques principales d'analyse de la sûreté de fonctionnement

A.1.1 Prévision du taux de défaillance

A.1.1.1 Description et objet

La prévision du taux de défaillance est une méthode applicable principalement au cours des phases d'étude et de conception initiale afin d'estimer le taux de défaillance des matériels et des systèmes. Cette méthode peut également être utilisée dans la phase de fabrication pour l'amélioration des produits.

Trois techniques de base peuvent être adoptées:

– prévision du taux de défaillance dans les conditions de référence, également appelée analyse « Parts count »;

– prévision du taux de défaillance dans les conditions d'exploitation, également appelée analyse « Parts stress »;

– prévision du taux de défaillance à l'aide de l'analyse de similarité.

Le choix de la technique à utiliser dépend du niveau de connaissance disponible du système au moment de la prévision effective de la fiabilité, et également du degré d'approximation acceptable.

A.1.1.2 Prévision du taux de défaillance dans les conditions de référence et dans les conditions d'exploitation

Dans les deux premiers cas, l'analyste doit connaître le nombre et le type de composants pouvant constituer le système. Il doit également connaître les conditions d'exploitation pour lesquelles la prévision du taux de défaillance est effectuée. Lorsque les conditions d'exploitation sont identiques aux conditions de référence pour les composants, il n'est alors pas nécessaire d'en tenir compte. Toutefois, lorsque la prévision du taux de défaillance s'applique à des conditions d'exploitation différentes des conditions de référence, les conditions d'application (électriques, thermiques, environnementales) spécifiques du composant concerné sont prises en considération en utilisant les modèles développés à cet effet. Une base de données fiable du taux de défaillance est nécessaire pour des prévisions exactes. La CEI 61709 donne des recommandations concernant la méthode d'évaluation des taux de défaillance dans des conditions appelées "conditions de référence" dans ce type de base de données, mais ne contient toutefois pas de données relatives au taux de défaillance. Plusieurs manuels relatifs aux données de taux de défaillance ont été élaborés, certains d'entre eux étant d'ailleurs disponibles dans le commerce. Cependant, les calculs de la fiabilité peuvent se révéler chronophages et des outils logiciels du commerce permettent par conséquent d'effectuer ces calculs.

La prévision du taux de défaillance repose sur les hypothèses suivantes:

– les composants sont reliés logiquement en série (c'est-à-dire que chacun d'entre eux est nécessaire pour le système);

– les taux de défaillance des composants sont constants dans la durée;

– les défaillances de composants sont indépendantes.

Ces hypothèses doivent être débattues en se référant au système étudié dans la mesure où elles peuvent aboutir à une estimation du cas le plus défavorable en cas de redondances aux niveaux d'assemblage les plus élevés.

L'hypothèse d'une constance des taux de défaillance réduit fortement l'effort de calcul, dans la mesure où le taux de défaillance total constitue simplement la somme des taux de défaillance des pièces. Ceci n'implique pas nécessairement que le taux de défaillance total est une caractéristique de fiabilité significative: les défaillances n'affectent pas tous les systèmes de la même manière. Les défaillances des éléments de diagnostic, ainsi que certains modes de panne, peuvent ne pas affecter la fonctionnalité du système. Dans ce cas, le taux de défaillance total fournit uniquement une mesure du nombre d'actions de maintenance correctives, que ces dernières soient ou non liées aux défaillances fonctionnelles du système.

La prévision de fiabilité d'un système génère des prévisions à un niveau de précision acceptable, selon les modèles disponibles de défaillance des composants. Le même principe s'applique lors du calcul de la prévision du taux de défaillance dans des conditions d'exploitation.

A.1.1.3 Prévision du taux de défaillance à l'aide de l'analyse de similarité

L'analyse de similarité comprend l'utilisation de données de performances des matériels mis en service qui permettent de comparer les matériels de nouvelle conception avec les matériels précédents en vue de la prévision de la fiabilité des entités finales.

Les mêmes données d'exploitation permettent d'effectuer des comparaisons de matériels similaires aux niveaux de l'entité finale, du sous-ensemble ou du composant, en appliquant toutefois des algorithmes et des facteurs de calcul différents aux divers éléments. Les éléments à comparer peuvent inclure:

– les conditions d'exploitation et environnementales (mesurées et spécifiées);
– les caractéristiques de conception;
– les processus de conception;
– les processus d'assurance de la fiabilité;
– les processus de fabrication;
– les processus de maintenance;
– les composants et les matériaux.

Pour chacun des éléments susmentionnés, il convient de comparer un certain nombre de sous-éléments. A titre d'exemples, les conditions d'exploitation et environnementales peuvent inclure une température en régime permanent, des variations de l'humidité et de la température, la puissance électrique, le cycle de service, les vibrations mécaniques, etc. Les caractéristiques de conception des matériels peuvent inclure le nombre de composants (séparés selon la famille des principaux composants), le nombre d'ensembles de cartes imprimées, la taille, le poids, les matériaux, etc.

Il convient que l'analyse de similarité inclue les algorithmes ou méthodes de calcul nécessaires utilisés pour quantifier les similarités et les différences entre les matériels évalués et les matériels précédents.

L'analyse de similarité des éléments est utilisée lorsqu'une analyse de similarité ne peut être effectuée du fait de l'absence ou de la non-disponibilité de tout matériel précédent suffisamment similaire pour une comparaison avec le matériel de conception nouvelle effectivement évalué. L'analyse de similarité des éléments constitue la comparaison structurée des éléments du nouveau matériel avec les éléments similaires de différents matériels précédents, pour lesquels des données de fiabilité sont disponibles.

A.1.1.4 Avantages

– La durée et le coût de l'analyse sont très réduits, sous réserve de la disponibilité des données et modèles de référence.

– Les informations et données d'entrée nécessaires sont peu nombreuses et adaptées par conséquent à la situation des premières phases de conception et de développement.

– On obtient des informations de base sur la fiabilité des composants dès le stade initial de la conception et du développement.

– Méthode adaptée à des calculs manuels et effectués sur ordinateur.

– Courte formation nécessaire.

A.1.1.5 Limites

– Il n'est pas possible de prendre en considération la structure fonctionnelle (par exemple, les redondances à un niveau inférieur). Par conséquent, seules des structures simples se prêtent à l'analyse « Parts count ».

– Le niveau de précision des prévisions peut être faible, notamment pour les petits sous-systèmes et les productions en faible quantité, dans la mesure où les données publiées ou recueillies sont valables uniquement d'un point de vue statistique, c'est-à-dire qu'elles exigent des échantillons de grande taille.

– Il est impossible d'évaluer les modes et mécanismes de défaillance, ainsi que leurs effets.

A.1.1.6 Normes

La norme CEI applicable est la CEI 61709.

A.1.1.7 Exemple pour un circuit intégré (tel que donné dans la CEI 61709)

Pour une mémoire RAM (vive) bipolaire, le taux de défaillance est indiqué sous la forme $\lambda_{\text{ref}} = 10^{-7}\ h^{-1}$ dans une base de données fiable établie sur les conditions de référence suivantes énoncées dans la CEI 61709.

– température ambiante de référence: $\theta_{\text{amb, ref}}$ 40°C;

– échauffement propre de référence: 20 °C.

Quelle est la valeur du taux de défaillance à une température ambiante de θ_{amb} = 70 °C avec le même échauffement propre?

Étape 1: Le modèle de taux de défaillance dans les conditions d'exploitation est indiqué dans la CEI 61709 sous la forme $\lambda = \lambda_{\text{ref}} \times \pi_{\text{T}}$.

Étape 2: A partir de la Figure A.1 (prise dans la CEI 61709), le facteur relatif à l'influence de la température devient π_{T} = 3,4,

– en utilisant la température virtuelle de référence de jonction
$\theta_1 = \theta_{\text{amb, ref}} + \Delta T_{\text{ref}}$ = 40 °C +20 °C = 60 °C,

– et la température virtuelle réelle de jonction
$\theta_2 = \theta_{\text{amb}} + \Delta T_{\text{ref}}$ = 70 °C + 20 °C = 90 °C.

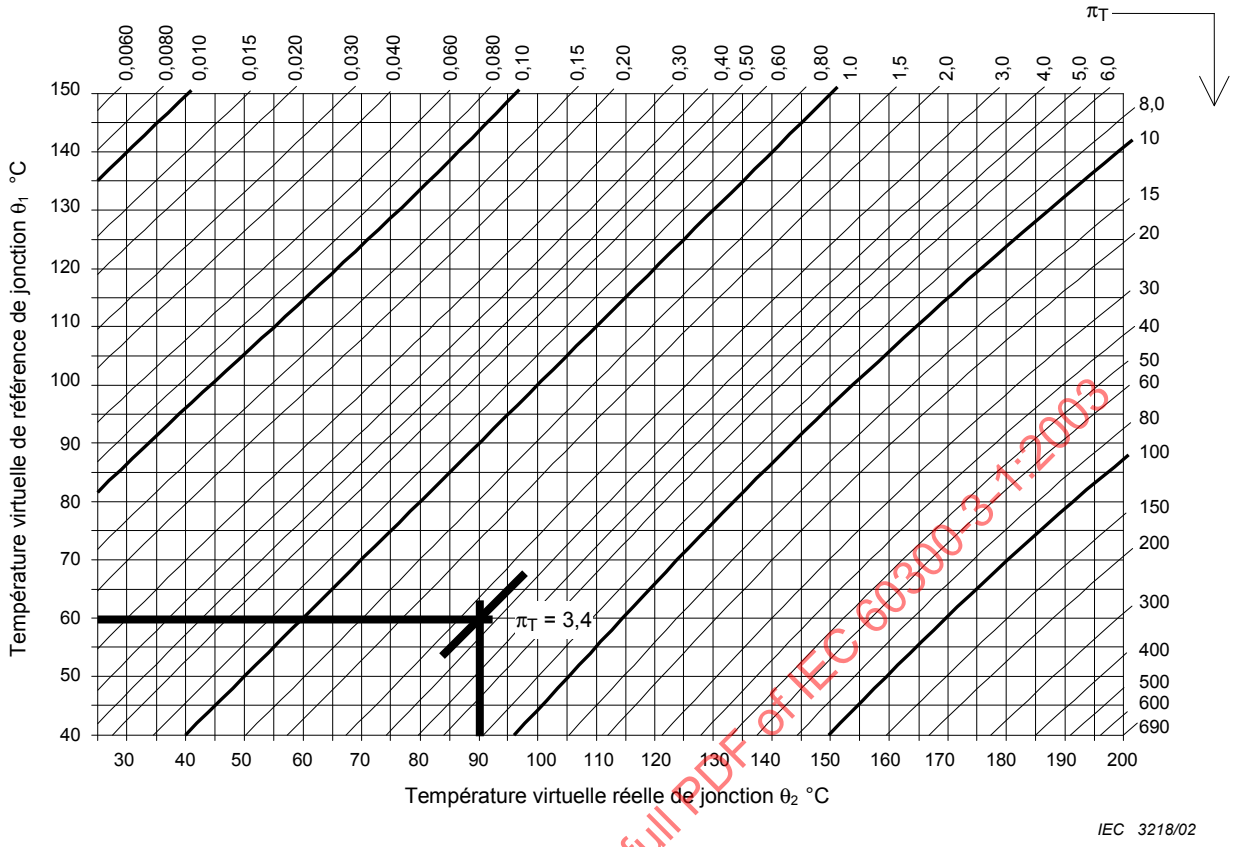


Figure A.1 – Dépendance à la température du taux de défaillance

Étape 3: Le taux de défaillance à $\theta_{amb} = 70\,°C$ est obtenu sous la forme $\lambda = \lambda_{ref} \times \pi_T = 10^{-7} h^{-1} \times 3{,}4 = 3{,}4 \times 10^{-7} h^{-1}$.

A.1.2 Analyse par arbre de panne (AAP)

A.1.2.1 Description et objet

L'analyse par arbre de panne (AAP) est une approche descendante qui permet d'analyser la sûreté de fonctionnement d'un produit. Elle se rapporte à l'identification et à l'analyse des conditions et facteurs produisant ou contribuant à produire une issue indésirable définie et qui affectent les caractéristiques de performance, de sécurité, d'économie ou d'autres caractéristiques spécifiées du produit.

L'AAP peut également être établie afin de fournir un modèle de prévision de fiabilité du système et de pouvoir réaliser des études de rentabilité dans une phase de conception du produit.

Utilisée comme outil de détection et d'évaluation quantitative d'une cause de panne, l'AAP représente une méthode efficace d'identification et d'évaluation des modes de défaillance et des causes des effets connus ou présumés.

Tenant compte des effets non favorables connus et de la capacité à trouver des modes et des causes de défaillance respectifs, l'AAP permet une réduction opportune des modes de défaillance potentiels, ce qui permet d'améliorer la sûreté de fonctionnement du produit dans sa phase de conception.

L'AAP, établie pour représenter l'architecture matérielle et logicielle, ainsi que pour traiter la fonctionnalité, et développée pour traiter par ailleurs des événements de base, devient une technique de modélisation de la fiabilité systématique qui tient compte des interactions

complexes des pièces du système, par une modélisation de leurs dépendances fonctionnelles ou de défaillance, des événements favorisant les défaillances, des événements de cause commune, ainsi que par la possibilité d'une représentation des réseaux.

Des méthodes telles que la réduction booléenne et l'analyse des coupes sont utilisées pour estimer la fiabilité et la disponibilité du système à l'aide de la technique AAP. Les données de base requises sont les taux de défaillance des composants, les taux de réparation, la probabilité d'occurrence des modes de panne, etc.

A.1.2.2 Application

L'analyse par arbre de panne a une double application, en tant que moyen d'identification de la cause d'une défaillance connue, et comme outil d'analyse d'un mode de défaillance, et de modélisation et prévision de la sûreté de fonctionnement.

L'AAP permet d'analyser les pannes potentielles, leurs modes et leurs causes, ainsi que de quantifier leur contribution à l'indisponibilité du système dans la phase de conception du produit. L'arbre de panne est construit de manière à représenter non seulement les fonctions du système, mais également les caractéristiques de leurs matériels et logiciels associées à leurs interactions. Lorsque le facteur humain fait partie intégrante du système, il est possible d'inclure également les erreurs humaines dans l'AAP. La probabilité d'occurrence des causes des modes de panne est déterminée par l'analyse d'ingénierie, puis synthétisée afin d'évaluer l'importance de leur contribution à la défiabilité globale du produit, ce qui permet une croissance de la rentabilité et de la fiabilité. Ceci permet une modélisation de la sûreté de fonctionnement d'une combinaison de matériels, électroniques et mécaniques, et logiciels, ainsi que leur interaction. Dans cette application, l'AAP devient un outil d'analyse puissant.

A.1.2.3 Eléments-clés

Les **éléments-clés** d'un arbre de panne sont les suivants

– portes et événements,
– coupes.

Les portes représentent l'issue et les événements représentent l'entrée dans les portes. La représentation symbolique de certaines portes spécifiques peut varier d'un manuel ou d'un logiciel d'analyse à l'autre, la représentation des portes de base est toutefois pratiquement universelle.

Les coupes sont des groupes d'événements qui, s'ils se produisent tous, provoquent la défaillance du système. Les coupes minimales contiennent le nombre minimal des événements nécessaires à la défaillance. La suppression de l'une de ces coupes entraînerait une non-défaillance du système.

A.1.2.4 Avantages

– Peut être initié dès les premières phases de conception, puis développé plus en détail conjointement au développement de la conception.
– Identifie et enregistre systématiquement les chemins logiques de panne en partant d'un effet spécifique pour remonter jusqu'aux causes originelles en utilisant l'algèbre de Boole.
– Permet de convertir facilement les modèles logiques en mesures de probabilité correspondantes.

A.1.2.5 Limites

– L'AAP n'est pas en mesure de représenter correctement la dépendance des événements en fonction du temps ou des séquences.

– L'AAP comporte des limites eu égard à la reconfiguration ou au comportement des systèmes dépendant de l'état.

Ces limites peuvent être compensées par une combinaison de l'AAP avec les modèles de Markov, où ces derniers sont pris comme événements de base dans les arbres de panne.

A.1.2.6 Exemple

Représentation par arbre de panne d'un système central pour un amplificateur audio: les sous-systèmes principaux sont les portes d'accès à la porte centrale et au système amplificateur.

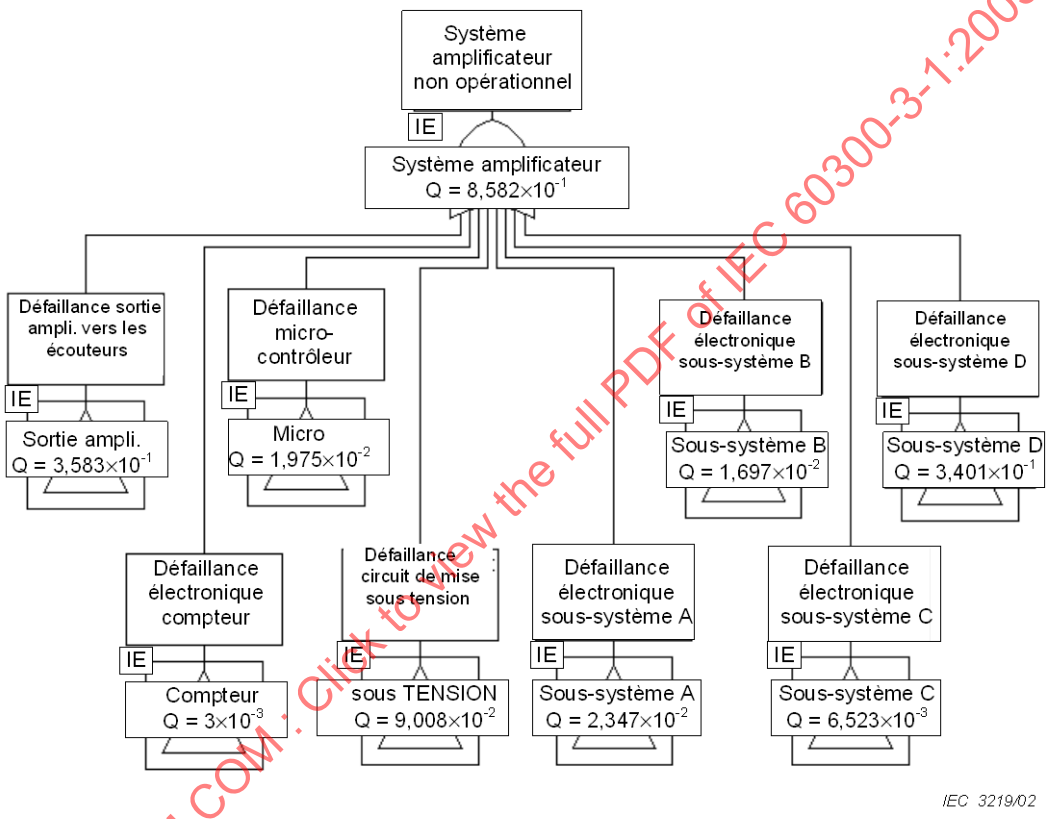


Figure A.2 – Arbre de panne pour un amplificateur audio

Le sous-arbre illustré à la Figure A.3 contribue le plus à la défaillance globale.

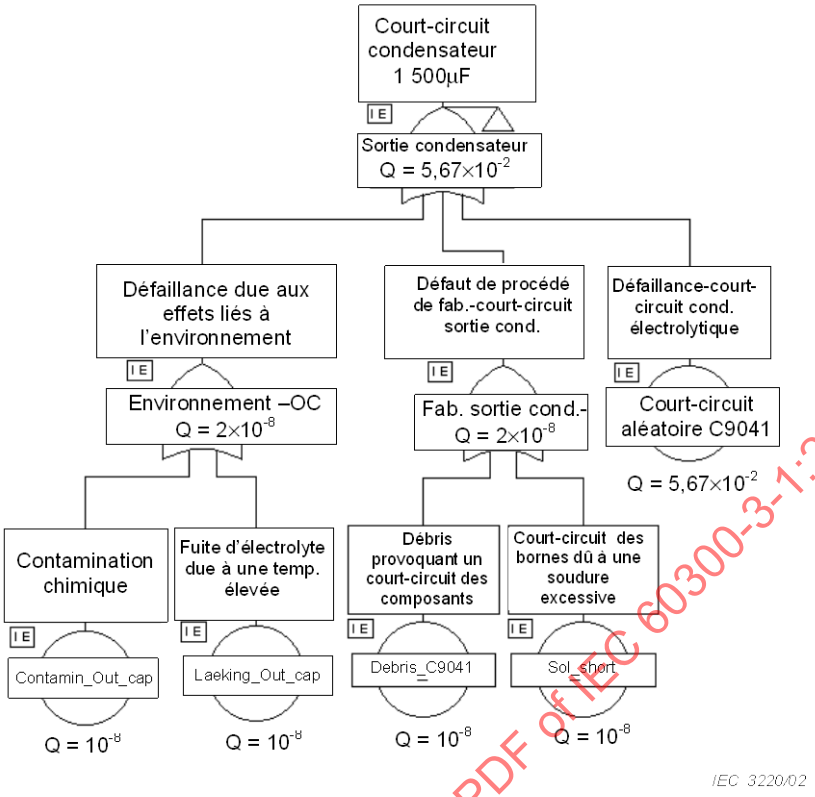
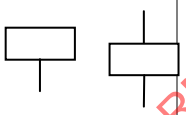


Figure A.3 – Sous-arbre issu de l'AAP de la Figure A.2

Les symboles donnés dans le Tableau A.1 sont utilisés dans la représentation de l'arbre de panne.

Tableau A.1 – Symboles utilisés dans la représentation de l'arbre de panne

Symbole AAP	Nom du symbole	Description
	EVENEMENT DE TETE ou EVENEMENT INTERMEDIAIRE	Événement central ou intermédiaire qui décrit la panne du système, la panne du sous-système ou une panne de niveau plus élevé que la panne du niveau de l'événement de base
	EVENEMENT DE BASE	Événement de base pour lequel il existe des informations concernant la fiabilité
	EVENEMENT NON DEVELOPPE	Partie du système qui doit encore être développée ou définie
	PORTE DE TRANSFERT	Porte indiquant que cette partie du système est développée dans une autre partie ou page du diagramme
	PORTE OU	Cet événement de sortie se produit si un au moins des événements d'entrée se produit
	Porte ET	L'événement de sortie se produit si tous les événements d'entrée se produisent

Cette analyse avait pour objectif de déterminer la cause la plus vraisemblable de défaillance de l'amplificateur. Le condensateur électrolytique placé sur la sortie de l'amplificateur en direction de l'écouteur contribue le plus à la défaillance de l'amplificateur. Il est fort probable que le taux de défaillance interne du condensateur génère sa mise en court-circuit. Cette situation se produit du fait que le condensateur de tension assignée inférieure a été choisi à l'origine pour le calcul en raison de sa taille plus petite, le déclassement de ce condensateur étant ainsi de 90 %, compte tenu de la seule tension c.c. Le courant ondulatoire ne constituait en rien une cause supplémentaire de défaillance du condensateur.

Les deux causes ont produit une augmentation d'un ordre de grandeur du taux de défaillance d'origine du condensateur qui n'est pas faible, compte tenu de la taille du condensateur électrolytique (1 500 µF), même avec un déclassement supérieur. On a ensuite remplacé le condensateur par un condensateur à tension assignée appropriée et, comme il apparaissait à six endroits dans la conception de l'amplificateur, ce remplacement a permis de réduire la probabilité globale de défaillance de l'amplificateur de plus de 20 % pour sa durée de vie prévisible prédéterminée. La réduction de la cause du mode de panne conduit à une amélioration de la fiabilité du système.

Dans le cas présent, l'indisponibilité du système, Q, calculée pour la durée de fonctionnement donnée, représente également la probabilité de défaillance du système, $F(t)$, étant donné que les temps de réparation n'étaient pas admis.

Les portes mentionnées dans l'exemple ci-dessus constituent des annotations de référence, à l'exception des portes qui représentent les sous-systèmes, où le triangle, qui représente les portes de transfert, indique un développement ultérieur de ces dernières, et où le carré, qui les délimite, indique que chacune de ces portes est illustrée sur une page séparée.

A.1.3 Analyse par arbre d'événement (AAE)

A.1.3.1 Description et objet

L'arbre d'événement considère un nombre de conséquences possibles d'un événement initiateur ou de la défaillance d'un système. Ainsi, il peut être combiné en toute efficacité avec un arbre de panne. La racine d'un arbre d'événement peut être considérée comme l'événement de tête d'un arbre de panne. On appelle parfois cette combinaison analyse des causes-conséquences, où l'AAP permet d'analyser les causes et l'AAE permet d'analyser les conséquences d'un événement initiateur. Afin d'évaluer le caractère sérieux de certaines conséquences d'un événement initiateur, il convient d'identifier et d'examiner toutes les voies de conséquence possibles, ainsi que de déterminer leur probabilité.

A.1.3.2 Application

L'analyse par arbre d'événement est effectuée lorsque l'examen de tous les parcours possibles des événements ultérieurs, de leur séquence, et des issue/conséquence les plus probables de l'événement initiateur constitue un élément essentiel. Après un événement initiateur, plusieurs événements/conséquences ultérieurs de premier ordre peuvent s'ensuivre. La probabilité associée à l'occurrence d'un parcours spécifique (séquence d'événements) représente le produit des probabilités conditionnelles de tous les événements survenant dans ce parcours.

A.1.3.3 Eléments-clés

L'initiateur (événement initiateur), les événements ultérieurs et les conséquences constituent les **éléments-clés** de l'application de l'AAE.

A.1.3.4 Avantages

Le principal avantage d'un arbre d'événement réside dans la possibilité d'évaluer les conséquences d'un événement, et ainsi de prévoir la limitation potentielle d'une conséquence défavorable mais non moins fortement probable. L'analyse par arbre d'événement présente

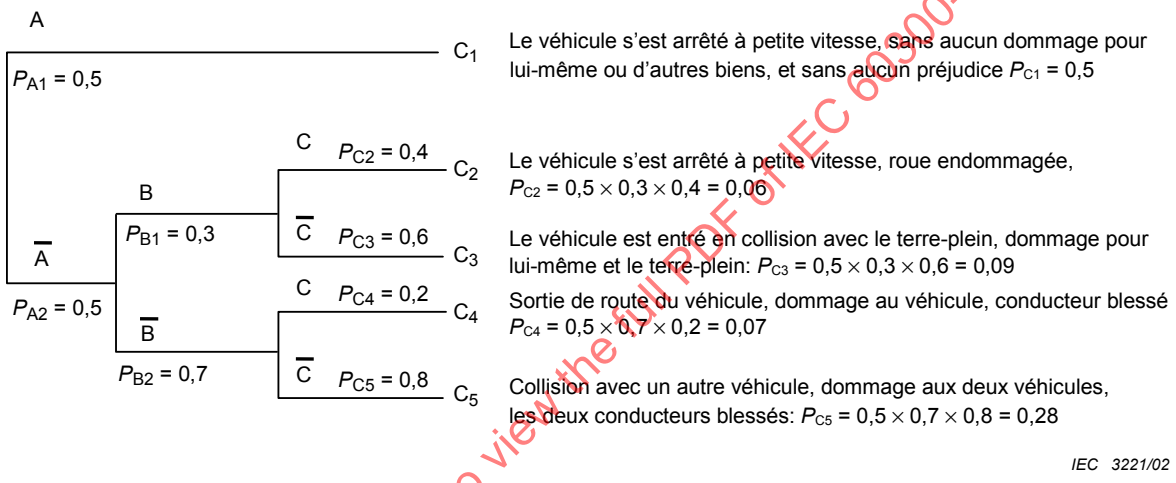
ainsi tous ses avantages lorsqu'elle est effectuée en complément de l'analyse par arbre de panne. L'analyse par arbre d'événement peut également être utilisée comme un outil dans l'analyse du mode de panne. Lorsqu'elle est ascendante, l'analyse suit les parcours possibles d'un événement (un mode de défaillance) afin de déterminer les conséquences probables d'une défaillance.

A.1.3.5 Limites

Une attention toute particulière doit être accordée au traitement approprié des probabilités conditionnelles et à l'indépendance des événements dans l'analyse par arbre.

A.1.3.6 Exemple

Un exemple d'arbre d'événement simple est donné à la Figure A.4. Cet exemple évalue l'issue d'un événement simple, à savoir la défaillance d'un pneumatique d'automobile, en examinant plusieurs issues possibles.



Légende

A = aucun dommage ou préjudice matériel

B = dommage matériel, aucun préjudice

C = dommage occasionné au seul véhicule, aucun autre dommage matériel

Figure A.4 – Arbre d'événement

A.1.4 Analyse par bloc-diagramme de fiabilité (BDF)

A.1.4.1 Description et objet

L'analyse par bloc-diagramme de fiabilité (BDF) est une méthode d'analyse du système. Un bloc-diagramme de fiabilité est la représentation graphique de l'organisation fonctionnelle d'un système en termes de sous-systèmes et/ou composants. Ainsi, on peut représenter les chemins de succès du système suivant la manière dont les blocs (sous-systèmes/composants) sont reliés entre eux.

A.1.4.2 Application

Les blocs-diagramme figurent parmi les premières tâches exécutées lors de la définition du produit. Il convient de les construire comme partie intégrante du développement du concept initial. Il convient de les utiliser dès que le programme a été défini, de les compléter comme partie intégrante de l'analyse des exigences, et de les développer de façon continue selon un niveau plus détaillé dans la mesure où l'on dispose des données nécessaires pour prendre des décisions et opérer des arbitrages.

A.1.4.3 Eléments-clés

On peut employer diverses techniques d'analyse qualitative pour obtenir un bloc-diagramme de fiabilité.

– Définir le succès d'un système.
– Diviser le système en blocs fonctionnels adaptés à l'objet de l'analyse de la fiabilité. Certains blocs peuvent correspondre à des sous-structures du système qui, à leur tour, peuvent être représentées par d'autres BDF (réduction du système).
– Effectuer des analyses qualitatives; il existe plusieurs méthodes d'évaluation quantitative d'un BDF. Suivant le type de structure (réductible, irréductible), on peut recourir à des techniques booléennes simples, des tables de vérité et/ou à l'analyse des chemins ou des coupes, pour prévoir les valeurs de la fiabilité et de la disponibilité du système en partant des données de base sur les composants.

A.1.4.4 Avantages

– Souvent établie presque directement à partir du diagramme fonctionnel du système; ceci présente l'avantage supplémentaire de réduire les erreurs de construction et/ou l'illustration systématique des chemins fonctionnels pertinents pour la fiabilité du système.
– Aborde la plupart des configurations de systèmes, y compris les chemins fonctionnels parallèles, redondants, en attente ou alternatifs.
– Peut être employée pour effectuer une analyse complète des variations et arbitrages concernant les modifications des paramètres de fonctionnement du système.
– Permet (dans l'application à deux états) un traitement relativement facile des chemins fonctionnels (ou non fonctionnels) pour obtenir des modèles logiques minimaux (par exemple, par l'algèbre de Boole).
– Peut servir pour les analyses de sensibilité en vue de mettre en évidence les éléments qui contribuent le plus à la fiabilité d'ensemble du système.
– Peut servir à élaborer des modèles permettant d'évaluer la fiabilité et la disponibilité d'ensemble du système en terme de probabilité.
– Donne des diagrammes compacts et concis pour un système entier.

A.1.4.5 Limites

– N'est pas, en elle-même, adaptée à l'analyse d'une défaillance spécifique. En d'autres termes, les chemins cause-effet(s) ou effet-cause(s) ne sont pas particulièrement mis en évidence.
– Exige un modèle probabiliste des performances de chaque élément du diagramme.
– Ne présente pas les sorties intempestives ou non prévues, à moins que l'analyste prenne des mesures particulières à cette fin.
– Est axée essentiellement sur l'analyse des succès et ne se prête pas vraiment à l'analyse des stratégies complexes de maintenance et de réparation ni à celle de la disponibilité globale.
– Se limite généralement aux systèmes non réparables.

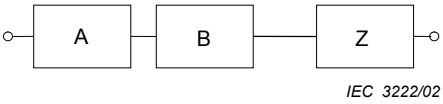
A.1.4.6 Normes

La norme CEI applicable est la CEI 61078.

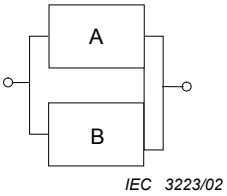
A.1.4.7 Exemple

Les modèles élémentaires (il convient que chaque bloc soit indépendant d'un autre bloc) sont illustrés à la Figure A.5.

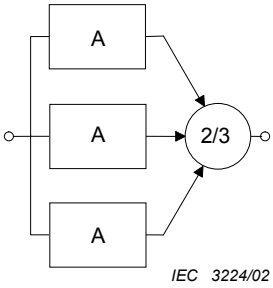
Série



Parallèle (redondance chaude)



Modèle m sur n



En attente (redondance froide)

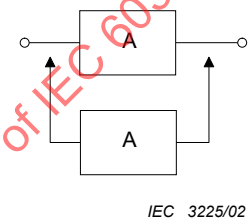


Figure A.5 – Modèles élémentaires

Des modèles plus complexes dans lesquels le même bloc apparaît à plusieurs reprises dans le diagramme peuvent être évalués grâce

– au théorème de probabilité totale;
– aux tables de vérité de Boole.

A.1.5 Analyse de Markov

A.1.5.1 Description et objet

La modélisation de Markov est une méthode probabiliste qui permet la dépendance statistique des caractéristiques de défaillance ou de réparation des composants individuels à adapter à l'état du système. De fait, la modélisation de Markov peut prendre en compte les effets des défaillances de composants dépendant de l'ordre et des variations des taux de transition produites par la contrainte ou d'autres facteurs. L'analyse de Markov est de ce fait une méthode adaptée à l'évaluation de la sûreté de fonctionnement de structures de systèmes à complexité fonctionnelle et de stratégies de réparation et maintenance complexes.

La méthode repose sur la théorie des chaînes de Markov. Pour les applications de sûreté de fonctionnement, le modèle de référence normal est le modèle de Markov à homogénéisation temporelle qui exige la constance des taux de transition (défaillance et réparation). Il est possible de calculer de manière approchée les transitions non exponentielles en recourant à une séquence de transitions exponentielles, en augmentant toutefois l'espace d'états. Pour ce modèle, il existe des techniques à solution numérique générales et efficaces, la seule limite à cette application étant la taille de l'espace d'états.

La représentation du comportement du système par un modèle de Markov exige de déterminer tous les états possibles du système, illustrés de préférence par un schéma dans un diagramme de transition d'état. De plus, les taux de transition (constants) d'un état à un autre (défaillance d'un composant ou taux de réparation, taux d'événements, etc.) doivent

être spécifiés. Les sorties typiques d'un modèle de Markov se traduisent par la probabilité d'être dans un ensemble d'états donné (cette probabilité est généralement la mesure de la disponibilité).

A.1.5.2 Application

Le domaine d'application approprié de cette technique est celui où les taux de transition (défaillance ou réparation) dépendent de l'état du système ou varient avec la charge, le niveau de contrainte, la structure du système (par exemple, en attente), la politique de maintenance ou d'autres facteurs. Notamment, la structure du système (redondance froide ou chaude, pièces de rechange) et la politique de maintenance (équipes de réparation uniques ou multiples) produisent des dépendances qui ne peuvent être identifiées par d'autres techniques à traitement informatique moins intensif.

Les prévisions de fiabilité/disponibilité constituent les applications typiques.

A.1.5.3 Eléments-clés

L'application de la méthodologie implique les étapes-clés suivantes:

– définition de l'espace d'états du système;
– affectation de taux de transition (dépendant du temps) entre les états;
– définition de mesures de sortie (regrouper les états qui provoquent une défaillance du système);
– génération du modèle mathématique (matrice de taux de transition) et résolution des modèles de Markov en recourant à un progiciel adapté;
– analyse des résultats.

A.1.5.4 Avantages

L'application de la méthodologie présente les avantages suivants:

– Elle fournit un modèle probabiliste souple permettant d'analyser le comportement du système.
– Elle est adaptable à des configurations redondantes et des politiques de maintenance complexes, à des modèles de traitement des pannes-erreurs complexes (pannes intermittentes, latence de pannes, reconfiguration), modes de fonctionnement dégradés et défaillances de cause commune.
– Cette méthodologie fournit des solutions probabilistes pour les modules à insérer dans d'autres modèles tels les blocs-diagrammes et les arbres de panne.
– Elle permet une modélisation précise des séquences d'événements avec un modèle spécifique d'ordre d'occurrence.

A.1.5.5 Limites

– Le nombre croissant des composants de système se traduit par une augmentation exponentielle du nombre d'états, conduisant à un travail d'analyse intensif.
– Les utilisateurs peuvent éprouver une certaine difficulté à élaborer et à vérifier le modèle, qui requiert un logiciel spécifique pour l'analyse.
– L'étape de solution numérique est disponible uniquement avec des taux de transition constants.
– La solution de référence du modèle de Markov ne permet pas d'obtenir immédiatement des mesures spécifiques, telles que les MTTF et MTTR, lesdites mesures exigeant toutefois une attention directe.

A.1.5.6 Normes

La norme CEI applicable est la CEI 61165.

A.1.5.7 Exemple

Un matériel (ou une unité) électronique contient une partie fonctionnelle (F) et une partie diagnostic (D) (voir Figure A.6). On entend par "diagnostic" les parties du système qui exécutent toutes les fonctions de surveillance, contrôle et affichage, par quelque moyen que ce soit (matériel, logiciel, micro-logiciel), ces parties étant également désignées comme "parties de surveillance".

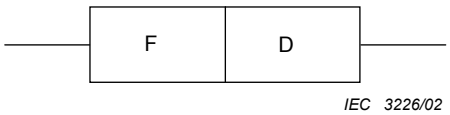


Figure A.6 – Exemple d'unité

La terminologie suivante est utilisée dans cet exemple:

défaut d'alarme
incapacité à déclencher une alarme en raison d'une panne dans la partie diagnostic

état d'indisponibilité
état d'une entité caractérisée soit par une panne, soit par une incapacité potentielle à exécuter une fonction requise lors d'une maintenance préventive

fausse alarme
panne signalée par un matériel de test intégré ou d'autres circuits de surveillance en l'absence de panne fonctionnelle

mode de panne
un des états potentiels d'une entité défaillante, pour une fonction requise donnée

couverture de pannes
pourcentage de pannes d'une entité pouvant être reconnu dans des conditions données

diagnostic de pannes
mesures prises pour la reconnaissance et la localisation des pannes, ainsi que pour l'identification des causes

panne latente
panne existante non encore reconnue

état de disponibilité
état d'une entité caractérisée par le fait qu'elle peut exécuter une fonction requise, en supposant l'existence effective des ressources externes, si nécessaire

Les modèles de fiabilité impliquent habituellement certaines simplifications: dans un bloc-diagramme, chaque bloc fonctionnel d'un schéma de même nature comporte deux états. Un état désigne un fonctionnement correct (état de disponibilité), l'autre état désignant une panne (état d'indisponibilité). Le modèle à deux états simplifie nettement l'analyse de fiabilité, mais n'est parfois pas adapté à la description de la situation effective dans le monde réel, dans lequel chaque bloc fonctionnel doit comporter une partie fonctionnelle (F) et une partie diagnostic (D), les deux parties peuvent par ailleurs présenter des défaillances. La modélisation de Markov permet de traiter de ces questions.

L'application de l'analyse de Markov exige avant tout de définir l'espace d'états du système. Les Tableaux A.2 et A.3 présentent les états d'une unité du monde réel et les effets des défaillances dans les états F et D.

Tableau A.2 – Etats de l'unité

Etat	Définition
1	Fonctionnement correct
2	Panne de diagnostic en mode de défaut d'alarme
3	Panne fonctionnelle couverte par diagnostic
4	Panne fonctionnelle non couverte par diagnostic (non détectable)
5	Panne fonctionnelle non détectée par diagnostic, défaillant en mode de défaut d'alarme
6	Panne de diagnostic en mode de fausse alarme

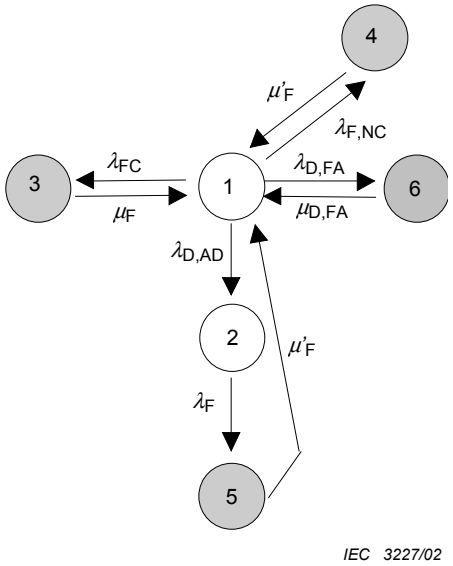
Tableau A.3 – Effets des défaillances dans les parties en mode fonctionnel et diagnostic

Etat de F	Etat de D	Etat	Effets
En fonctionnement	En fonctionnement	1	Fonctionnement correct (état 1)
En fonctionnement	Panne en mode de fausse alarme	6	Émission de l'alarme. F en état de disponibilité jusqu'à ce que le personnel de maintenance effectue une réparation. Généralement, lorsque F n'est pas redondante, le système la laisse normalement en service (état 6) jusqu'à ce que la réparation intervienne.
	Panne en mode de défaut d'alarme	2	Pas d'émission d'alarme. La partie F est dans l'état de disponibilité (état 2) jusqu'à ce qu'elle présente une défaillance (état 5)
Panne	En fonctionnement	3	Émission de l'alarme. Reconnaissance de panne correcte (état 3)
Panne	Panne	5	Séquence d'événements permettant d'atteindre cet état: Panne de diagnostic (mode de défaut d'alarme), le sous-système passe dans l'état 2 Panne fonctionnelle, pas d'émission d'alarme (état 5)
Panne	Absence	4	Panne non détectable (état 4)

La Figure A.7 illustre le diagramme de transition d'état associé et reconnaît que

– la partie fonctionnelle peut ne pas être couverte par diagnostic: cela signifie qu'une défaillance de la partie fonctionnelle peut ne pas être détectée (état 4),

– la partie diagnostic peut omettre d'émettre une alarme, lorsqu'il convient que cette omission ne soit pas effective (état 6) ou peut ne pas émettre d'alarme lorsqu'il convient qu'elle en émette une (états 2 et 5).



NOTE Les états à cercle blanc sont les états de disponibilité, tandis que les états à cercle gris sont les états d'indisponibilité.

Figure A.7 – Diagramme de transition d'état

Les taux de transition (dépendant du temps) entre les différents états sont présentés dans le Tableau A.4.

Tableau A.4 – Taux de transition

λ_F	Taux de défaillance de F, partie fonctionnelle
$\lambda_{F,C}$	Taux de défaillance de F couvert (défaillances détectables par diagnostic)
$\lambda_{F,NC}$	Taux de défaillance de F non couvert (noter que $\lambda_F = \lambda_{F,C} + \lambda_{F,NC}$)
$\lambda_{D,AD}$	Taux de défaillance de D en mode de défaut d'alarme
$\lambda_{D,FA}$	Taux de défaillance de D en mode de fausse alarme (noter que $\lambda_D = \lambda_{D,AD} + \lambda_{D,FA}$)
μ_F	Taux de réparation après une panne mise en évidence par diagnostic
μ'_F	Taux de réparation après une panne non mise en évidence par diagnostic
$\mu_{D/FA}$	Taux de réparation après une panne en mode de fausse alarme

Une fois définis le diagramme d'état et les taux de transition, il est possible de calculer la disponibilité grâce à un progiciel adapté. Une analyse des paramètres peut également être facilement réalisée, compte tenu des variations des taux de transition.

A.1.6 Analyse par réseau de Pétri

A.1.6.1 Description et objet

Les réseaux de Pétri constituent un outil graphique utilisé pour la représentation et l'analyse des interactions logiques complexes entre les composants ou les événements d'un système. La concurrence, le conflit, la synchronisation, l'exclusion mutuelle et la limite des ressources constituent les interactions complexes typiques qui font naturellement partie intégrante du langage des réseaux de Pétri.

Un graphique de réseau de Pétri représente la structure statique du système modélisé. Ce graphique est constitué de trois éléments primitifs:

– les places (habituellement sous la forme de cercles) qui représentent les conditions dans lesquelles le système peut se trouver;

– les transitions (habituellement sous la forme de barres) qui représentent les événements susceptibles de modifier une condition en une autre;

– les arcs (sous forme de flèches) qui relient les places aux transitions et inversement, et qui représentent les connexions admissibles logiques entre les conditions et les événements.

Une condition est valide dans une situation donnée si la place correspondante est marquée, c'est-à-dire si elle contient au moins un jeton • (sous forme de point noir). La dynamique du système est représentée par le mouvement des jetons sur le graphique. Une transition est activée si ses places d'entrée contiennent au moins un jeton. Une transition activée peut générer un tir, et la transition effectuant ce tir retire un jeton de chaque place d'entrée et en place un dans chaque place de sortie. La distribution des jetons dans les places s'appelle le marquage. En commençant par un marquage initial, l'application des règles d'activation et de tir produit tous les marquages accessibles appelés ensemble d'accessibilité des réseaux de Pétri. L'ensemble d'accessibilité fournit tous les états que le système peut atteindre à partir d'un état initial.

Les réseaux de Pétri classiques ne comportent pas la notion de temps. De nombreuses extensions existent toutefois dans lesquelles une temporisation se superpose au réseau de Pétri. Lorsqu'un taux d'activation (tir) constant est affecté à chaque transition, la dynamique des réseaux de Pétri peut être analysée au moyen d'une chaîne temporelle de Markov continue dont l'espace d'états est isomorphe à l'ensemble d'accessibilité du réseau de Pétri correspondant.

Le réseau de Pétri peut servir de langage évolué permettant de générer des modèles de Markov, plusieurs outils de l'analyse de la sûreté de fonctionnement sont par ailleurs basés sur cette méthodologie.

Les réseaux de Pétri fournissent également un environnement naturel de simulation.

A.1.6.2 Application

L'utilisation des réseaux de Pétri est recommandée lorsque des interactions logiques complexes doivent être prises en compte (concurrence, conflit, synchronisation, exclusion mutuelle, limite des ressources). Par ailleurs, ces réseaux constituent habituellement un langage plus facile et naturel qui permet de décrire un modèle de Markov.

A.1.6.3 Eléments-clés

L'élément-clé de l'analyse par réseau de Pétri est une description de la structure d'un système et de son comportement dynamique en termes d'éléments primitifs (places, transitions, arcs et jetons) du langage de réseau de Pétri; cette étape requiert l'utilisation d'outils logiciels ad hoc:

a) analyse qualitative structurelle;

b) analyse quantitative: lorsque des taux d'activation (tir) constants sont affectés aux transitions de réseau de Pétri, il est possible d'effectuer l'analyse quantitative en utilisant la solution numérique du modèle de Markov correspondant; dans le cas contraire, la simulation est la seule technique viable.

A.1.6.4 Avantages

Les réseaux de Pétri permettent de représenter des interactions complexes entre les modules matériels ou logiciels que d'autres techniques ne permettent pas de modéliser facilement.

Les réseaux de Pétri constituent un vecteur viable de génération de modèles de Markov. En règle générale, la description du système par un réseau de Pétri exige bien moins d'éléments que la représentation de Markov correspondante.

La représentation du réseau de Pétri permet de générer automatiquement le modèle de Markov, et la complexité de la procédure de solution analytique est dissimulée au modélisateur qui interagit uniquement au niveau du réseau de Pétri.

De plus, les réseaux de Pétri permettent une analyse structurale qualitative établie uniquement sur la propriété du graphique. Cette analyse structurale est, généralement, moins coûteuse que la génération du modèle de Markov, et fournit des informations utiles pour valider la cohérence du modèle.

A.1.6.5 Limites

Dans la mesure où l'analyse quantitative est basée sur la génération et la solution du modèle de Markov correspondant, la plupart des limites sont partagées avec l'analyse de Markov.

La méthodologie des réseaux de Pétri exige l'utilisation d'outils logiciels (plusieurs d'entre eux sont disponibles, développés par des organismes universitaires et industriels).

A.1.6.6 Exemple

Un système informatique multi-processeurs tolérant aux pannes, dont le schéma fonctionnel est illustré à la Figure A.8, contient deux sous-systèmes indépendants S_1 et S_2 avec une mémoire commune partagée M_3.

Chaque sous-système S_i (i = 1; 2) est constitué d'un processeur P_i, d'une mémoire locale M_i et de deux unités de disques dupliquées D_{i1} et D_{i2}. Un bus unique N relie les deux sous-systèmes et la mémoire commune partagée.

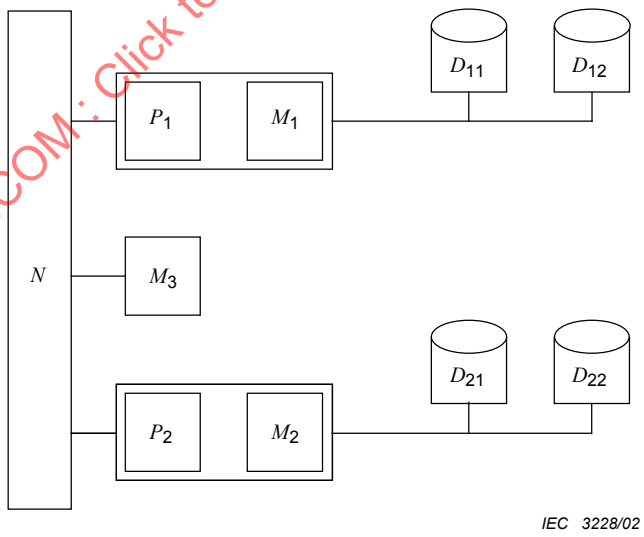


Figure A.8 – Schéma fonctionnel d'un système multi-processeurs

La représentation GSPN (réseau de Pétri stochastique généralisé) du système de la Figure A.8 est illustrée à la Figure A.9.

Les places dont les noms comportent le suffixe *.dn* modélisent les composants dans l'état de non-fonctionnement.

Un jeton dans la place S.*dn* modélise la défaillance globale du système.

Les transitions dont les noms comportent le suffixe *.f* modélisent la défaillance d'un composant.

Le marquage initial du réseau représente le système multi-processeurs dont tous les composants sont opérationnels.

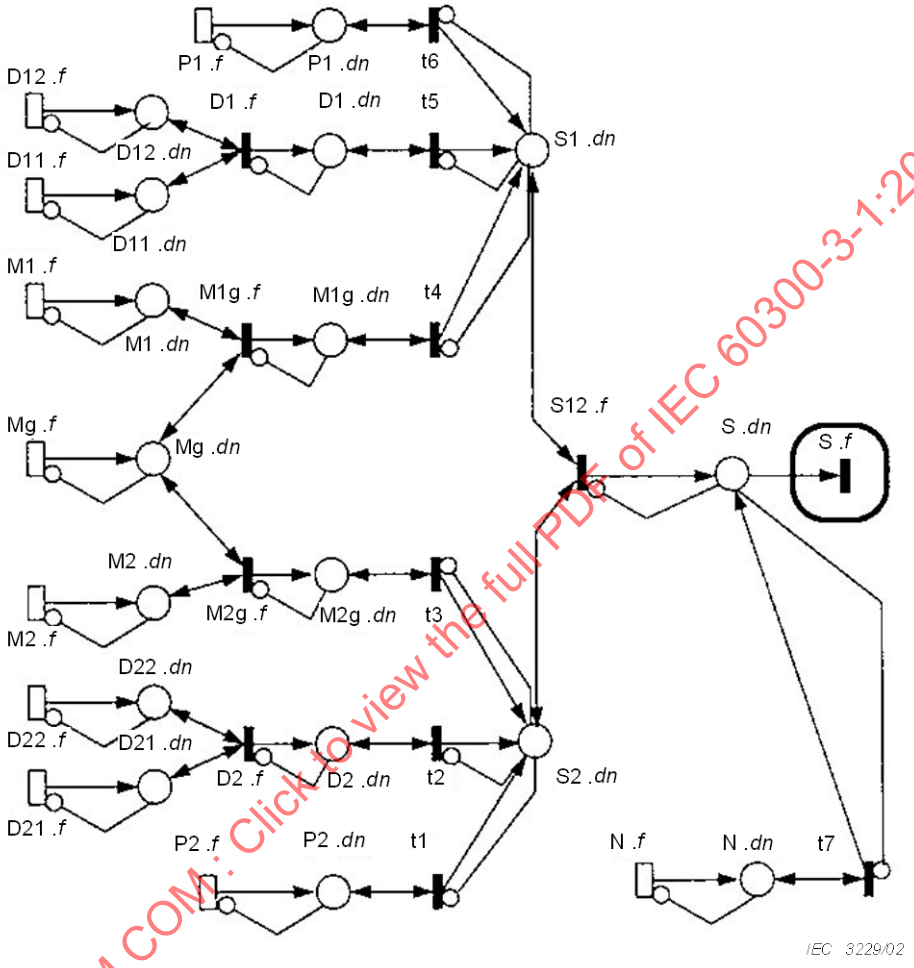


Figure A.9 – Réseau de Pétri d'un système multi-processeurs

A.1.7 Analyse des modes de défaillance et de leurs effets (AMDE)

A.1.7.1 Description et objet

L'analyse des modes de défaillance et de leurs effets (AMDE) est une méthode d'analyse de la sûreté de fonctionnement qualitative, de la base au sommet, particulièrement adaptée à l'étude des défaillances des matériaux, composants et équipements ainsi qu'à l'étude de leurs effets sur le niveau de système fonctionnel immédiatement supérieur. Les itérations de cette étape (identification des modes de défaillance unique et évaluation de leurs effets sur le niveau de système fonctionnel immédiatement supérieur) aboutissent à l'identification éventuelle de tous les modes de défaillance unique du système. L'AMDE se prête à l'analyse des systèmes de différentes technologies (électriques, mécaniques, hydrauliques, logiciel, etc.) caractérisées par des structures fonctionnelles simples. L'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) constitue une extension de l'AMDE destinée à inclure l'analyse de la criticité par une quantification des effets de la défaillance en

termes de probabilité d'occurrence et de gravité des effets éventuels. La gravité des effets est évaluée par référence à une échelle spécifiée.

A.1.7.2 Application

Les AMDE ou AMDEC sont généralement effectuées lorsque l'on prévoit un niveau de risque dans un programme donné dès la phase de développement d'un produit ou d'un processus. Les facteurs susceptibles d'être pris en compte sont les nouvelles technologies, les nouveaux processus ou les nouvelles conceptions, voire les modifications au niveau de l'environnement, des charges ou des réglementations. Ces analyses peuvent être réalisées sur des composants ou des systèmes qui constituent des produits, des processus ou des matériels de fabrication. Elles peuvent également être effectuées sur des systèmes logiciels.

A.1.7.3 Eléments-clés

L'analyse AMDE ou AMDEC suit généralement les étapes suivantes:

– identification de la manière dont il convient que le composant du système fonctionne;
– identification des modes de défaillance potentiels, ainsi que des effets et des causes;
– identification du risque lié aux modes de défaillance et à ses effets;
– identification des actions recommandées pour éliminer ou réduire le risque;
– actions de suivi pour exécuter les mesures recommandées.

A.1.7.4 Avantages

– Identifie systématiquement les relations entre cause et effet.
– Donne une indication initiale des modes de défaillance susceptibles d'être critiques, notamment des défaillances uniques qui peuvent se propager.
– Identifie les issues générées par des causes spécifiques ou les événements initiateurs que l'on considère importants.
– Fournit un cadre d'identification des mesures destinées à limiter le risque.
– Sert à l'analyse préliminaire de systèmes ou de processus nouveaux ou qui n'ont pas été éprouvés.

A.1.7.5 Limites

– Les données de sortie peuvent être nombreuses même pour des systèmes relativement simples.
– Peut devenir compliquée et inexploitable à moins qu'il n'existe une relation assez directe (ou "chaîne directe") entre la cause et l'effet.
– Peut difficilement traiter les séquences temporelles, les processus de rétablissement, les conditions ambiantes, les aspects de maintenance, etc.
– La priorisation de la criticité des modes est compliquée du fait des facteurs concurrentiels impliqués.

A.1.7.6 Normes

La norme CEI applicable est la CEI 60812.

A.1.7.7 Exemple

Un exemple d'analyse des modes de défaillance et de leurs effets est donné dans le Tableau A.5.

Tableau A.5 – Exemple d'AMDE

Niveau d'intervention: N° de fiche: Phase de mission					Conception par: Entité: Version:				Préparé par: Approuvé par: Date:			
Réf. entité	**Description / fonction de l'entité**	**Code d'entrée de défaillance**	**Mode de défaillance**	**Causes de défaillance possibles**	**Symptôme détecté**	**Effet local**	**Effet sur la sortie de l'unité**	**Disposition de compensation contre la défaillance**	**Classe de sévérité**	**Taux de défaillance**	**Source de données**	**Recommandations et mesures prises**
1.1.1	Stator du moteur	1111	Circuit ouvert	Rupture du bobinage	Rugosité à faible vitesse	Faible puissance	Déclenchement	Déclenchement de la protection en température mono-phase	4			
		1112	Circuit ouvert	Rupture de connexion	Rugosité à faible vitesse	Faible puissance	Déclenchement	Déclenchement de la protection en température mono-phase	3			
		1113	Rupture d'isolation	Défaut de fabrication à température élevée persistant	Système de protection	Surcharge	Pas de sortie	Inspection annuelle du dispositif de déclenchement en température	4			
		1114	Circuit ouvert de thermistance	Vieillissement, rupture de connexion	Système de protection	Aucun	Pas de sortie	Pièce de rechange correspondante	3			Recommande la connexion d'une pièce de rechange par le boîtier extérieur
		1115	Court-circuit de la thermistance	Système de protection	Système de protection	Marge de déclenchement réduite	Pas de sortie lorsque la charge est élevée	Déclencheur en température en rechange	3			Recommande la connexion d'une pièce de rechange par le boîtier extérieur
1.1.2	Système de refroidissement du moteur	1121	Refroidissement inapproprié	Basse pression différentielle de blocage	Haute température du stator détectée par la thermistance	Température excessive du bobinage	Température excessive du moteur	Déclenchement en température du stator	2			
		1122	Fuite dans l'atmosphère	Raccordement de tuyauterie	Température du moteur	Refroidissement inapproprié du moteur	Température excessive du moteur	Déclenchement en température, à vérifier toutes les 2 h	2			
		1122	Fuite venant de l'atmosphère	Raccordement de tuyauterie	Faible rendement	Air dans le circuit (système)	Aucun	A vérifier toutes les 2 h	2			
1.1.3	Roulement moteur	1131	Fuite externe des joints	Défaillance des paliers par usure	Carter d'huile de graissage à faible niveau	Perte d'huile de graissage	Aucun(e) à moins que la fuite ne soit importante	Contrôle quotidien	3			

A.1.8 Études de danger et d'exploitabilité (HAZOP)

A.1.8.1 Description et objet

Une étude HAZOP est un processus détaillé d'identification des dangers et des problèmes d'exploitabilité, exécuté par une équipe. L'étude HAZOP traite de l'identification des écarts éventuels par rapport à la conception attendue, de l'examen de leurs causes possibles et de l'évaluation de leurs conséquences.

Le socle d'une étude HAZOP est un « examen à base de mots-guides » constituant une recherche volontaire des écarts par rapport à la conception attendue. Cette dernière correspond au comportement souhaité ou spécifié par le concepteur pour un système, ses éléments et ses caractéristiques. Pour faciliter l'examen, un système est divisé en parties de manière à pouvoir définir correctement la conception attendue pour chaque partie. la conception attendue pour une partie donnée d'un système est exprimée en termes d'éléments qui véhiculent les caractéristiques essentielles de ladite partie et qui représentent ses divisions naturelles. Les éléments peuvent être des étapes ou des phases discrètes d'une procédure, des signaux individuels et des matériels d'un système de commande, des matériels ou des composants d'un processus ou d'un système électronique, etc.

Un processus d'interrogation utilisant des « mots-guides » prédéterminés permet d'identifier les écarts par rapport à l'intention de concept. Le terme directif est destiné à stimuler la réflexion imaginative, à focaliser l'étude et à susciter des idées et autres discussions, en augmentant de ce fait les opportunités d'exhaustivité de l'étude. Les termes directifs et leurs significations sont indiqués dans les Tableaux A.6 et A.7.

Tableau A.6 – Mots-guides de base et leurs significations génériques

Mots-guides	Signification
Non ou Pas	Négation totale de l'intention de concept
Plus	Augmentation quantitative
Moins	Baisse quantitative
Ainsi que	Modification/augmentation qualitative
Partie de	Modification/baisse qualitative
Inverse	Opposé logique de l'intention de concept
Autre que	Substitution totale

Tableau A.7 – Mots-guides supplémentaires relatifs au temps d'horloge et à l'ordre ou la séquence

Mots-guides	Signification
Tôt	Par rapport au temps d'horloge
Tard	Par rapport au temps d'horloge
Avant	Par rapport à l'ordre ou à la séquence
Après	Par rapport à l'ordre ou à la séquence

A.1.8.2 Application

Une étude HAZOP est adaptée surtout aux dernières phases de la conception détaillée pour un examen des installations d'exploitation, et lorsque des modifications sont apportées aux installations existantes. Le meilleur moment pour réaliser une étude HAZOP est juste avant de figer la conception.

A.1.8.3 Eléments-clés

– L'examen est un processus créatif.

– Il utilise de manière systématique une série de mots-guides afin d'identifier les écarts potentiels par rapport à la conception attendue et se sert de ces écarts comme "dispositifs déclencheurs" destinés à stimuler les membres des équipes à envisager de quelle manière l'écart pourrait se produire et quelles pourraient en être les conséquences.

– L'examen est effectué sous la direction d'un chef d'études formé et expérimenté, qui doit assurer une couverture complète du système à l'étude, en faisant appel à une réflexion analytique logique.

– L'examen repose sur des spécialistes de disciplines diverses ayant des compétences et une expérience appropriées, qui démontrent par ailleurs de l'intuition et un jugement sûr.

– Il convient que cet examen ait lieu dans une atmosphère de réflexion positive et de discussion franche. Tout problème identifié est consigné en vue d'une évaluation et d'une résolution ultérieures.

– Les solutions apportées aux problèmes identifiés ne constituent pas l'objectif principal de l'étude HAZOP, mais lorsqu'elles sont effectives, elles sont consignées afin que les concepteurs en tiennent compte.