

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2003 IEC, Geneva, Switzerland

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

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

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

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

IEC Central Office
3, rue de 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It also gives information on projects, replaced and withdrawn publications.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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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
CODE PRIX

XA

ICS 03.120.30; 21.020

ISBN 978-2-83220-664-5

Warning! Make sure that you obtained this publication from an authorized distributor.

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	6
3 Definitions	7
4 Basic dependability analysis procedure	8
4.1 General procedure	8
4.2 Dependability analysis methods	9
4.3 Dependability allocations.....	11
4.4 Dependability analysis.....	12
4.5 Maintenance and repair analysis and considerations	14
5 Selecting the appropriate analysis method	14
Annex A (informative) Brief description of analysis techniques.....	17
Bibliography.....	60
Figure 1 – General dependability analysis procedure	8
Figure A.1 – Temperature dependence of the failure rate.....	20
Figure A.2 – Fault tree for an audio amplifier	22
Figure A.3 – Sub-tree from FTA in Figure A.2	23
Figure A.4 – Event tree	25
Figure A.5 – Elementary models	27
Figure A.6 – Example of unit.....	29
Figure A.7 – State-transition diagram.....	30
Figure A.8 – Block diagram of a multiprocessor system	33
Figure A.9 – Petri net of a multiprocessor system	34
Figure A.10 – The HAZOP study procedure	39
Figure A.11 – Human errors shown as an event tree	43
Figure A.12 – Example – Application of stress–strength criteria	45
Figure A.13 – Truth table for simple systems	46
Figure A.14 – Example	46
Figure A.15 – Cause and effect diagram	58
Table 1 – Use of methods for general dependability analysis tasks	10
Table 2 – Characteristics of selected dependability analysis methods.....	16
Table A.1 – Symbols used in the representation of the fault tree	23
Table A.2 – States of the unit.....	29
Table A.3 – Effects of failures in functional and diagnostic parts	30
Table A.4 – Transition rates	31
Table A.5 – Example of FMEA	36
Table A.6 – Basic guide words and their generic meanings.....	37
Table A.7 – Additional guide words relating to clock time and order or sequence	37
Table A.8 – Credible human errors	42
Table A.9 – Truth table example	47

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

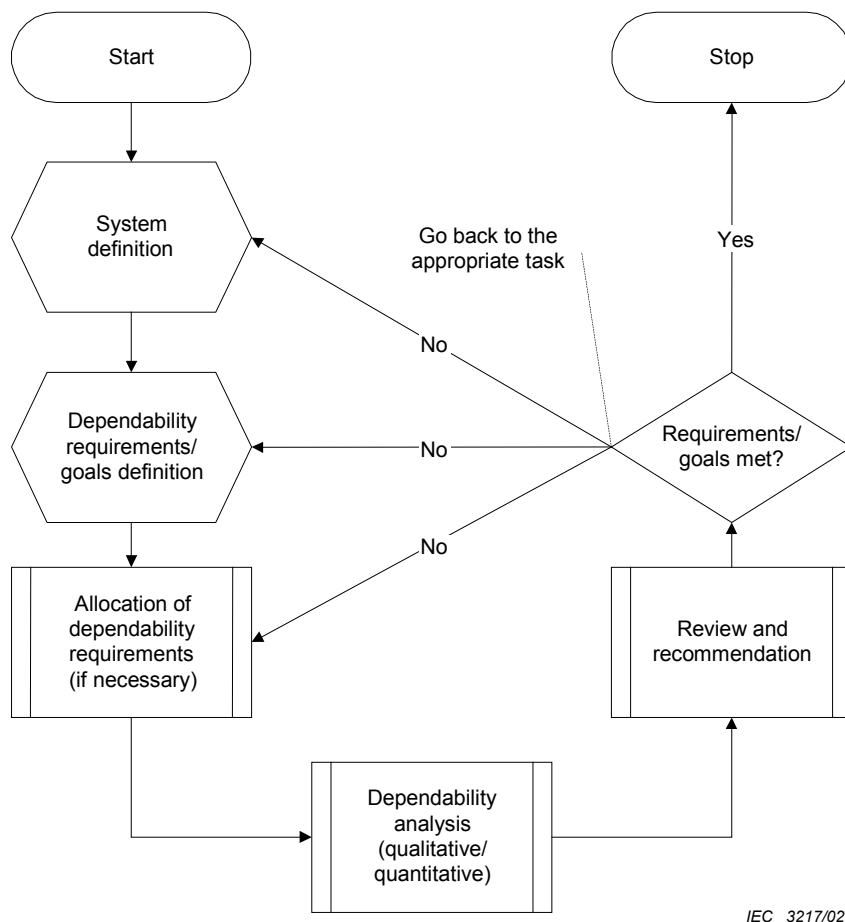


Figure 1 – General dependability analysis procedure

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 recommendations	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 dependability 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 $\lambda_{\text{ref}} = 10^{-7} \text{ h}^{-1}$ in a trustworthy database based on the following reference conditions stated in IEC 61709:

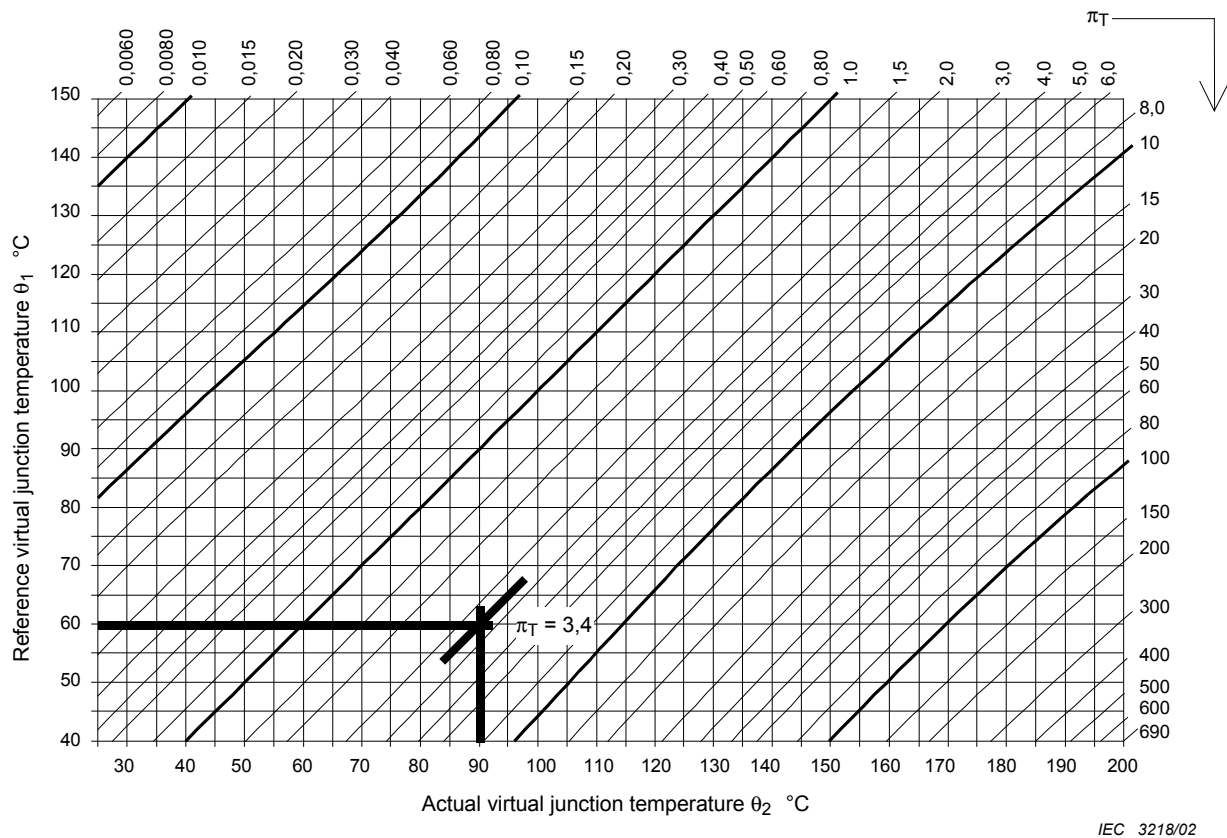
- reference ambient temperature: $\theta_{\text{amb, ref}}$ of 40 °C;
- reference self-heating: 20 °C.

What is the value of the failure rate at an ambient temperature of $\theta_{\text{amb}} = 70 \text{ °C}$ 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 $\pi_T = 3,4$,

- using the reference virtual junction temperature
 $\theta_1 = \theta_{\text{amb, ref}} + \Delta T_{\text{ref}} = 40 \text{ °C} + 20 \text{ °C} = 60 \text{ °C}$,
- and the actual virtual junction temperature
 $\theta_2 = \theta_{\text{amb}} + \Delta T_{\text{ref}} = 70 \text{ °C} + 20 \text{ °C} = 90 \text{ °C}$.



IEC 3218/02

Figure A.1 – Temperature dependence of the failure rate

Step 3: The failure rate at $\theta_{amb} = 70\text{ °C}$ 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.

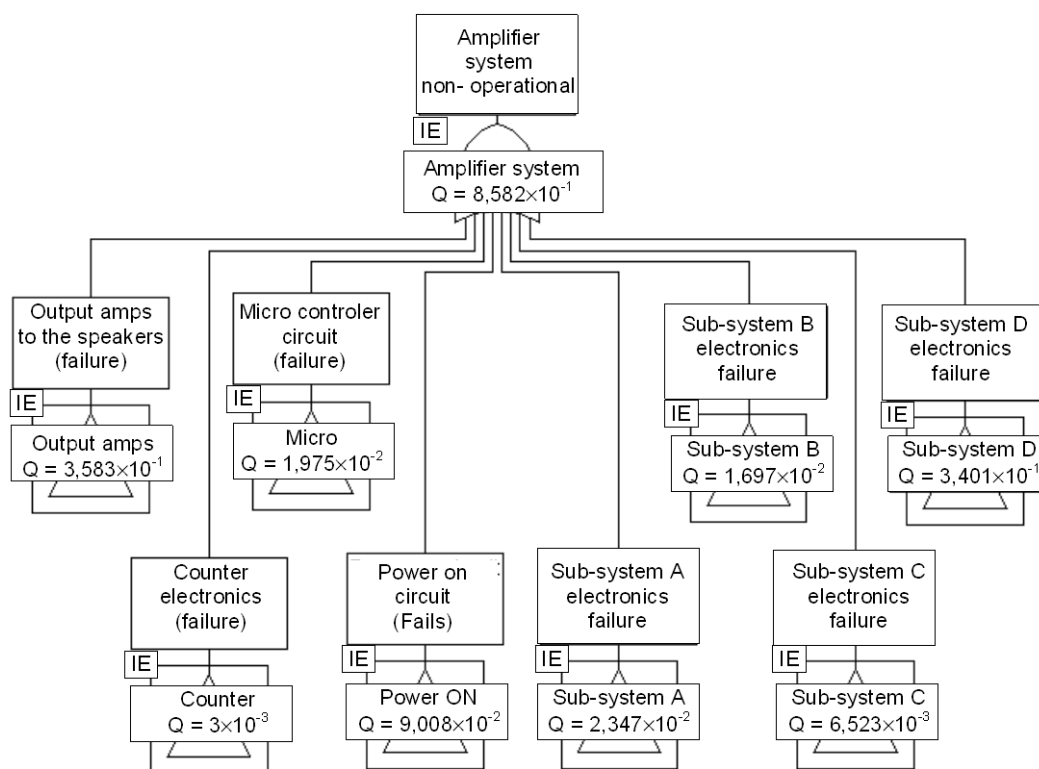
A.1.2.5 Limitations

- 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 be compensated by combination of FTA with Markov models, where Markov models are taken as basic events in fault trees.

A.1.2.6 Example

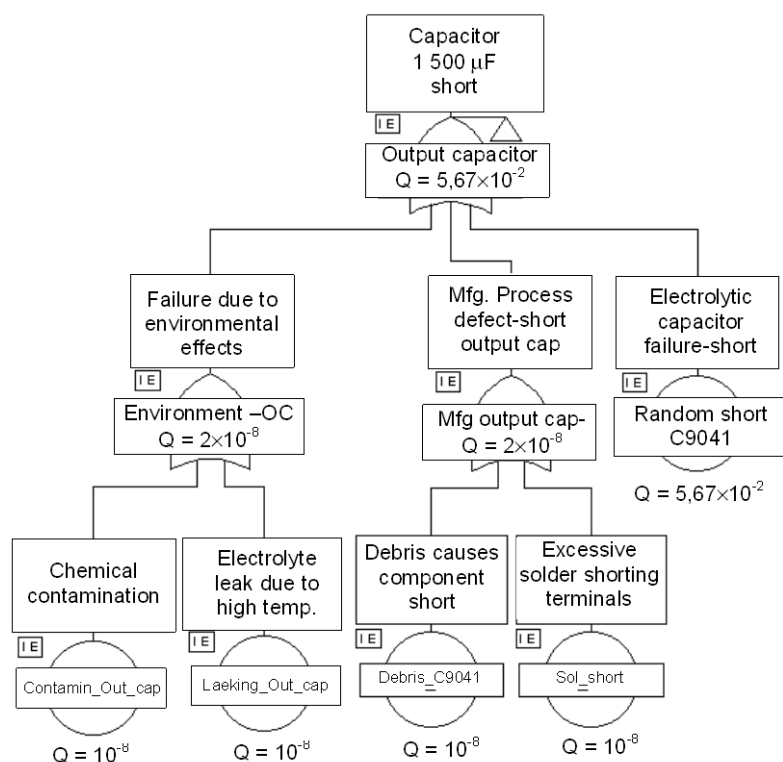
Top level system fault tree representation for an audio amplifier: the major sub-systems are the entry gates to the top-level gate and the amplifier system.



IEC 3219/02

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.



IEC 3220/02

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 tree

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 μ F) 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

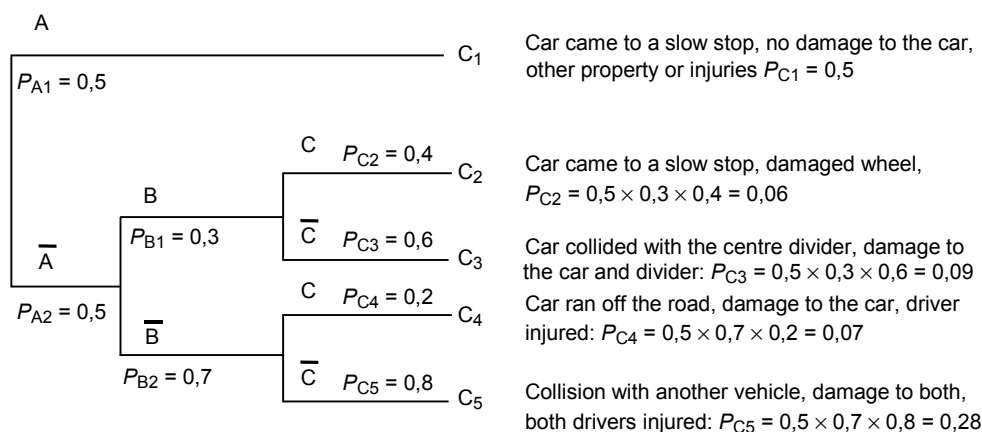
The major benefit of an event tree is the possibility to evaluate consequences of an event, and thus provide for possible mitigation of a highly probable, but unfavourable consequence. The event tree analysis is thus beneficial when performed as a complement to the fault tree analysis. The event tree 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.



IEC 3221/02

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.

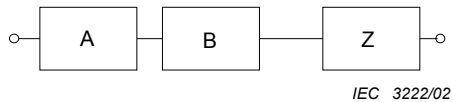
A.1.4.6 Standards

The applicable IEC standard is IEC 61078.

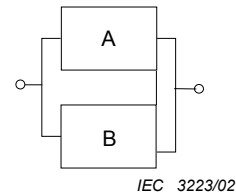
A.1.4.7 Example

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

Series



Parallel (active)



Model m out of n

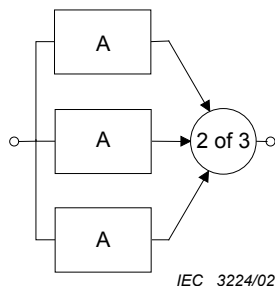
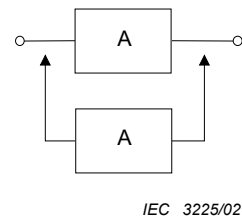
Standby
(cold standby)

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

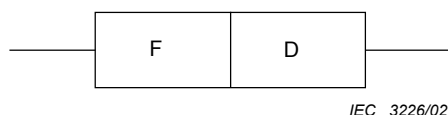
- As the number of system components increases, there is an exponential growth in the number of states resulting in labour intensive analysis.
- The model can be difficult for users to construct and verify, and requires specific software for the analysis.
- The numerical solution step is available only 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

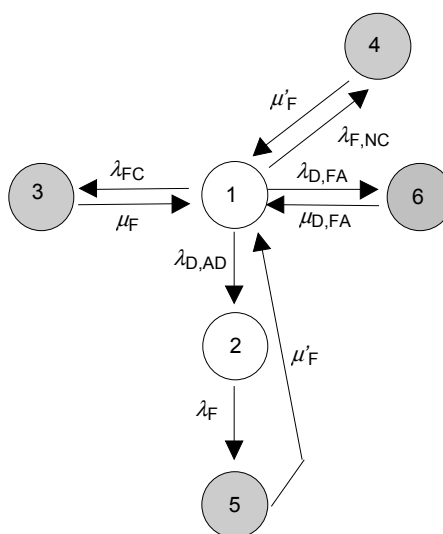
State	Definition
1	Correct operation
2	Diagnostic fault in alarm defection mode
3	Functional fault covered by diagnostics
4	Functional fault not covered by diagnostics (not detectable)
5	Functional fault not detected by diagnostics failed in alarm defection mode
6	Diagnostic fault in false alarm mode

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).



IEC 3227/02

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

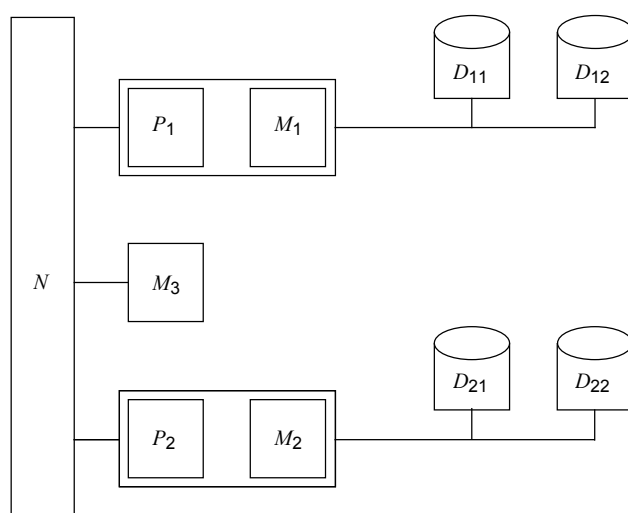
Since the quantitative analysis is based on the generation and solution of the corresponding Markov model, most of the limitations are shared with the Markov analysis.

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.



IEC 3228/02

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.

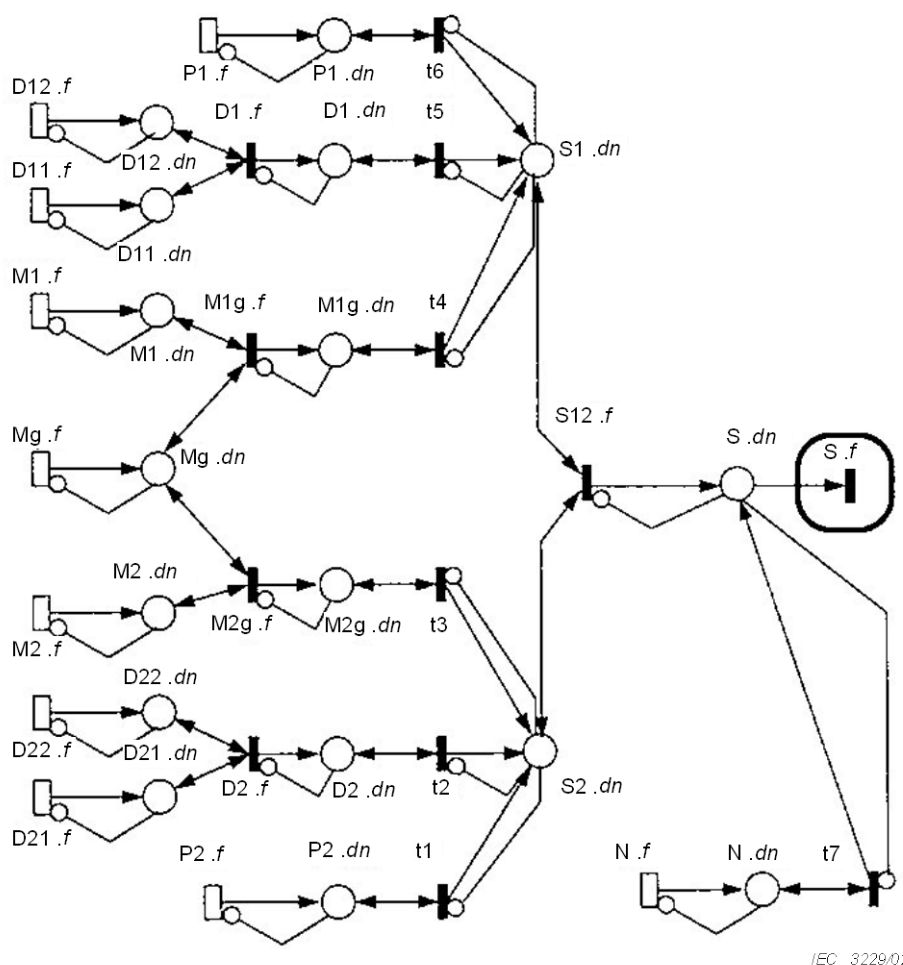


Figure A.9 – Petri net of a multiprocessor system

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. manufacturing 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
1.1.2	Motor cooling system	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
		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			
1.1.3	Motor bearing	1122	Leakage from atmosphere	Piping connection	Low output	Air in system	None	Check every 2 h	2			
		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