

Dependability management —

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

The European Standard EN 60300-3-1:2004 has the status of a
British Standard

ICS 03.120.30; 21.020

National foreword

This British Standard is the official English language version of EN 60300-3-1:2004. It is identical with IEC 60300-3-1:2003.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

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

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 57, two Annex ZA pages and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments
15370	29 September 2004	Implementation of the European Standard

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 26 March 2003

© BSI 29 September 2004

**Dependability management
Part 3-1: Application guide –
Analysis techniques for dependability –
Guide on methodology
(IEC 60300-3-1:2003)**

Gestion de la sûreté de fonctionnement
Partie 3-1: Guide d'application -
Techniques d'analyse de la sûreté
de fonctionnement –
Guide méthodologique
(CEI 60300-3-1:2003)

Zuverlässigkeitsmanagement
Teil 3-1: Anwendungsleitfaden –
Verfahren zur Analyse der Zuverlässigkeit -
Leitfaden zur Methodik
(IEC 60300-3-1:2003)

This European Standard was approved by CENELEC on 2004-09-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of the International Standard IEC 60300-3-1:2003, prepared by IEC TC 56, Dependability, was submitted to the formal vote and was approved by CENELEC as EN 60300-3-1 on 2004-09-01.

The following dates were fixed:

- | | | |
|--|-------|------------|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2005-09-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2007-09-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 60300-3-1:2003 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 60300-2	NOTE	Harmonized as EN 60300-2:1996 (not modified).
-------------	------	---

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

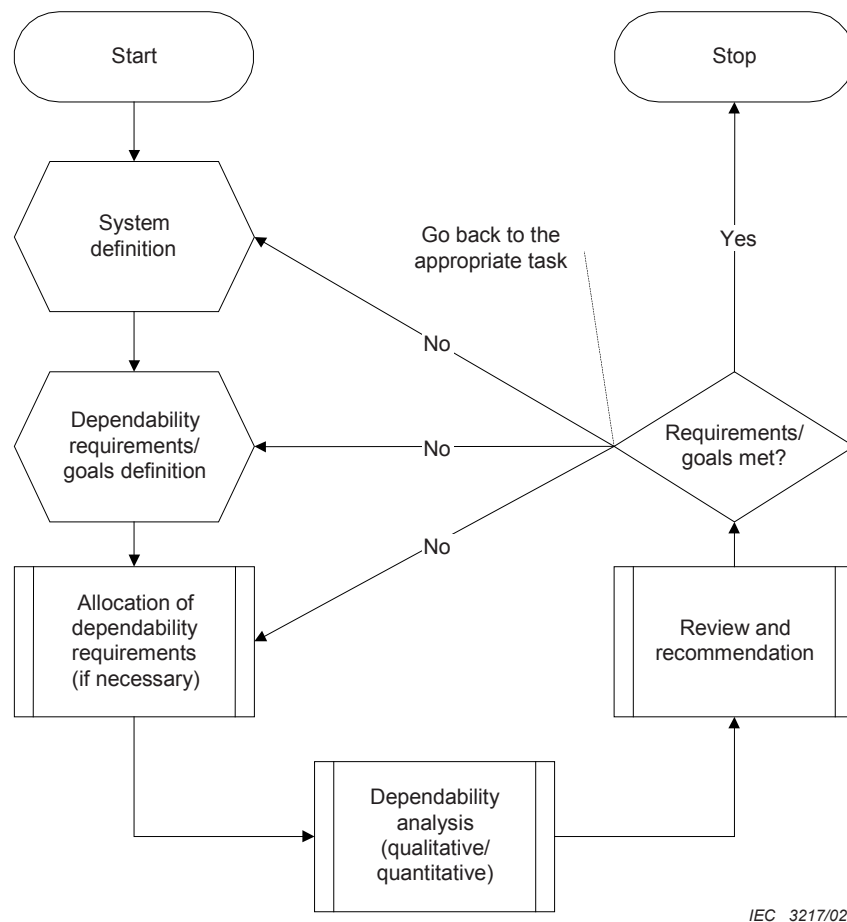


Figure 1 – General dependability analysis procedure

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:

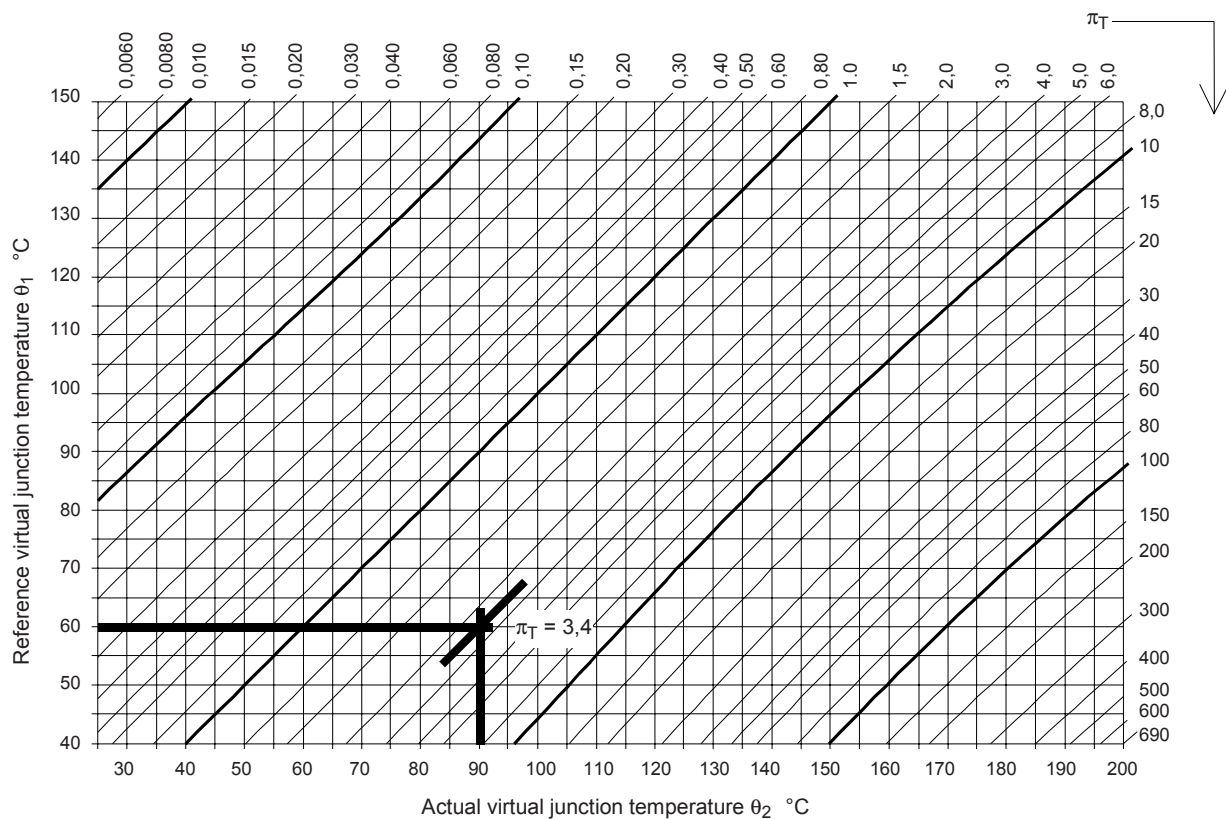
- reference ambient temperature: $\theta_{\text{amb, ref}}$ of 40 °C;
- reference self-heating: 20 °C.

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

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.