IEC 60706-5

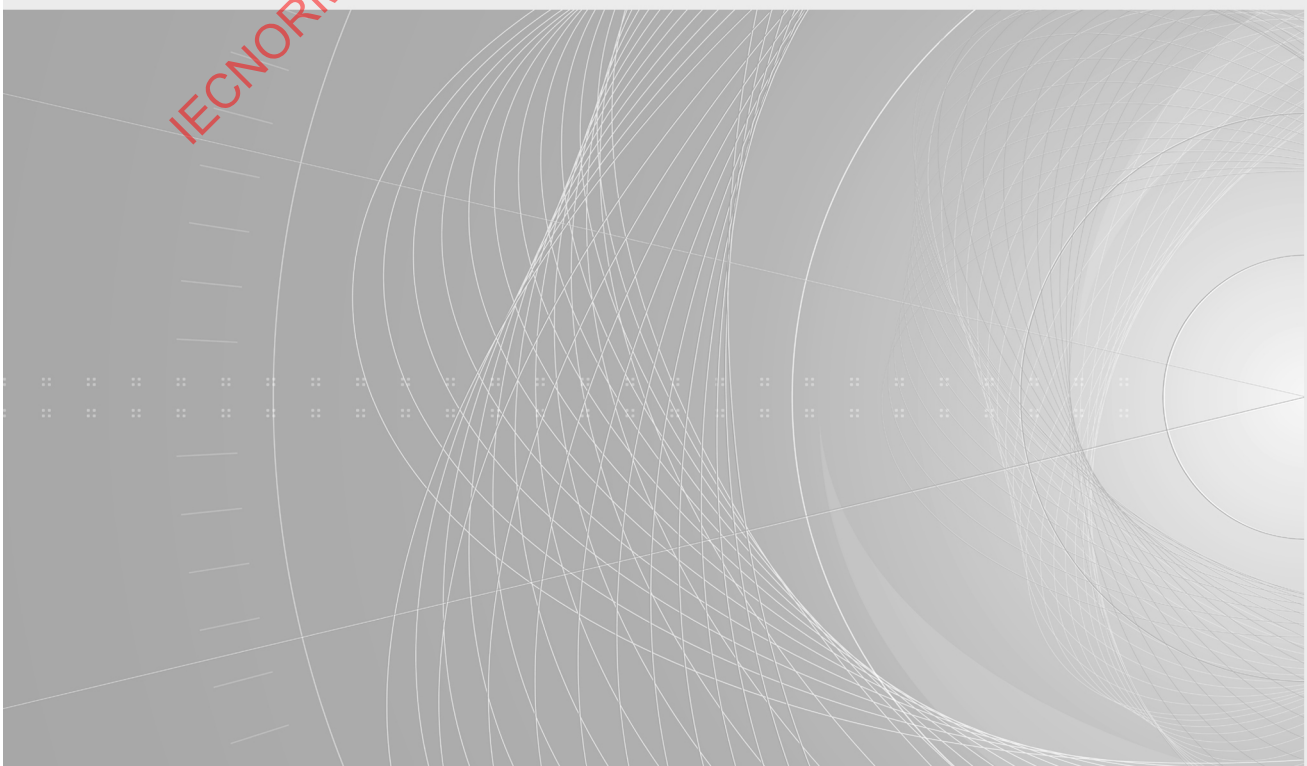
Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Maintainability of equipment –
Part 5: Testability and diagnostic testing

Maintenabilité de matériel –
Partie 5: Testabilité et tests pour diagnostic



IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60706-5

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Maintainability of equipment –
Part 5: Testability and diagnostic testing

Maintenabilité de matériel –
Partie 5: Testabilité et tests pour diagnostic

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 03.120.01; 03.120.30; 21.020

ISBN 2-8318-9295-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MAINTAINABILITY OF EQUIPMENT –

Part 5: Testability and diagnostic testing

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60706-5 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition published in 1994. This second edition constitutes a technical revision. It expands and provides more detail on the techniques and systems broadly outlined in the first edition.

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

FDIS	Report on voting
56/1211/FDIS	56/1231/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all the parts in the IEC 60706 series, under the general title *Maintainability of equipment*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

Testability is an important feature in the operation and maintenance of a system or equipment and has a significant effect on its availability and maintainability. Diagnostic testing may be carried out manually or with test equipment which may contain various levels of automation. Optimum design for testability requires close cooperation between design, operation and maintenance organizations. This standard is intended to highlight the various aspects of testability and diagnostic testing and to assist in their timely coordination.

In this standard, items to be considered in respect of their testability design may be systems, equipment or functional units which are the objects of a contract, and will be referred to as "products". Each product has to perform its required functions which should be verified during the development and production phases and should be retained over the whole life cycle. For a product to retain its functionality, the functional status of each sub-function should be known at any time while the product is in its operating condition. If a failure occurs, action should be taken to ensure that the fault is recognized and the faulty item localized. This requirement placed on the testability of a product might appear to be quite simple, but if it is not considered at the start of product development, subsequent realization will result in increased work and significantly increased cost. If all requirements are available at the start of development, the development engineer can specify the functional characteristic "testability" without much additional effort and therefore achieve considerable cost savings e.g. by minimizing the number of test steps for verifying the development results. Experience has shown that the extra cost and effort in the development phase can be recovered for example in the production phase since available test equipment can be used. Reliable fault recognition and low in-service maintenance costs increase the market value of a testable product considerably.

As the technologies which are applied in the products covered by this standard are wide-ranging, this document has been written in a neutral manner with regard to technologies and techniques. This standard therefore only provides an assessment basis for making calculations and the basic approach for achieving the required testability of a product. The technical realization of fault recognition and fault localization in the product is the task of the product development engineer and has to be achieved according to the state of the art at the time when the product is being developed. It is therefore not of great importance whether the required test task is realized in hardware or software form, but it is essential that all functions are checked via test paths and that the characteristic values established for testability correspond to the specified target values. If there are deviations from the target values, action should be taken to ensure that the target values are met. These actions should take place at an early stage of development before freezing the design.

MAINTAINABILITY OF EQUIPMENT –

Part 5: Testability and diagnostic testing

1 Scope

The purpose of this part of IEC 60706 is to

- provide guidance for the early consideration of testability aspects in design and development;
- assist in determining effective test procedures as an integral part of operation and maintenance.

This International Standard can be applied to all types of products which may include commercial off-the-shelf (COTS) items. In this respect, it does not matter whether the product belongs to mechanical, hydraulic, electrical or some other technology. In addition, this International Standard applies to the development of any products, with the aim of designing the product characteristics so that they are verifiable (testable).

The objective of this International standard is to ensure that prerequisites relating to the testability of products are defined in the preliminary phases of development, laid down by the customer, implemented, documented and verified during development.

This International Standard also provides methods to implement and assess testability as an integral part of the product design. It recommends that the product testability documentation should be continually updated over the product's life cycle.

2 Normative references

The following 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, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

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

3 Terms, definitions and acronyms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions of IEC 60050-191 apply together with the following:

3.1.1
built-in test
BIT
integrated capability of a test item enabling automatic fault recognition and fault localization

3.1.2
built-in test equipment
BITE
hardware and/or software assigned to the built-in test

3.1.3
commercial off-the-shelf
COTS
designates items readily available commercially

3.1.4
criticality
significance attached to a malfunction

NOTE Criticality is expressed in grades: the higher the grade, the more severe the consequences to be expected from the malfunction.

3.1.5
depth of test
specification of the level to which the unit or sub-unit is to be identified

3.1.6
design level
level to which the design elements (functional and/or physical units), when they already exist, are assigned within the product breakdown structure

NOTE In some cases “design level” is known as “indenture level”.

3.1.7
diagnosis correctness
proportion of faults of an item that can be correctly diagnosed under given conditions

3.1.8
diagnostic testing
test procedure carried out in order to make a diagnosis

3.1.9
false alarm
indication of failure which, after carrying out failure finding activities, is not found

3.1.10
false alarm rate
the percentage of false alarms in the total number of failure indications

3.1.11
fault recognition time
period of time between the instant of failure and fault recognition

3.1.12
fault simulation
inclusion of faults by non-destructive interventions in the hardware units and/or, where necessary, simulation via software in order to verify the diagnostic capability

3.1.13
function
performance required of the item

NOTE A function is always associated if realised with an item of a given level in the product breakdown structure.

3.1.14
functional model
conceptual representation of an item describing the interrelationship and dependencies between its stimuli and measurement (response) terminals

NOTE The functional model, which arises during the development of a product, is in principle a block diagram showing the functions of the product and supplemented to include the test paths envisaged by the developer.

3.1.15
functional test
testing of all the specified functions of hardware units to prove their functional capability

3.1.16
hardware unit
design element which represents functions and/or sub-functions in the form of hardware, possibly including software components

3.1.17
line replaceable unit
LRU
replaceable hardware or software unit which can be replaced directly on the equipment by the user or by a maintenance support facility

3.1.18
maintenance concept
interrelationship between the design levels and the levels of maintenance to be applied for the maintenance of an item

3.1.19
maintenance policy
general approach to the provision of maintenance and maintenance support based on the objectives and policies of owners, users and customers

3.1.20
monitoring
automatic supervision of the functions required for the operation in a selected operational mode; operation should not be affected by this

3.1.21
operational context
circumstances in which an item is expected to operate

3.1.22
parameter
physical quantity that specifies a function

3.1.23
product
specified deliverable goods or service

NOTE 1 In the context of dependability, a product may be simple (e.g. a device, a software algorithm) or complex e.g. a system or an integrated network comprising of hardware, software, human elements, support facilities and activities).

NOTE 2 Product has its own life cycle phases.

NOTE 3 Product has the same definition as item.

3.1.24
product breakdown structure
hierarchical tree visualizing the physical composition of a product by assemblies of units and sub-units

3.1.25
shop replaceable unit
SRU
replaceable hardware or software unit which can be replaced by the user depot/workshop or by the maintenance support facility at the same level or in the company's workshops

3.1.26
signal
variation of a physical quantity used to represent data

NOTE A signal is represented by one or several parameters.

3.1.27
specification
detailed definition of the functions of an item for a given level of the product breakdown structure

NOTE Specifications should be derived from the systems requirements and be verifiable.

3.1.28
statement of work
SoW
document which defines goods and services to be provided.

NOTE The statement of work is prepared or accepted by the customer and defines the work for which a contract is to be placed and which is to be provided by the contractor. It therefore forms the main technical document according to which the bidders present their offers, the contractor performs the work and the customer accepts the goods and services provided.

3.1.29
stimulus
input signal with defined parameters for the purpose of triggering functions

3.1.30
sub-function
sub-division of a function (see also function, 3.1.13)

3.1.31
terminal
generic term for the physical access points to the signals of a test item. Examples of physical implementations or relevant terms for synonymous expressions are

– pin

– connector
– plug/plug-type connector
– test point
– interface
– port

NOTE A terminal is generally identified by a unique identifier.

3.1.32
test concept
description of the results of the system testability requirements analysis and stipulation of the method of how the requirements are to be met

3.1.33
test coverage
ratio of the number of faulty functions actually capable of diagnosis by the given test instruction to the total number of functions

3.1.34
test equipment
tools (hardware and/or software) required for conducting tests

NOTE Due to the technology involved, these are divided into internal (BITE) and external test equipment.

3.1.35
test instruction
document describing how the tests required in the test specification are to be implemented

3.1.36
test path
description of the assignment of hardware units to their terminals, taking the associated test steps into account

NOTE In addition, the test path defines the (functional) relationship between the stimulus and the response.

3.1.37
test sequence
series of test steps

3.1.38
test specification
document in which test sequences, parameters and functions are specified

3.1.39
test step
smallest unit in a test conducted on a hardware unit

3.1.40
test task
sum of all the tests necessary to meet the specifications of fault recognition and localization

3.1.41
testability
design characteristic which determines the degree to which an item can be functionally tested under stated conditions

3.2 Acronyms

ATE	automatic test equipment
ATS	automatic testing system
BIT	built-in test
BITE	built-in test equipment
COTS	commercial off-the-shelf
DP	data processing
FL	fault localization
FM	functional monitoring
FME(C)A	failure mode, effects, (and criticality) analysis
FR	fault recognition
FT	functional test
FTA	fault tree analysis
HWE	hardware unit
LCC	life cycle cost
LORA	level of repair analysis
LRU	line replaceable unit
PCB	printed circuit board
SoW	statement of work
SRU	shop replaceable unit
SF	sub-function
TS	technical specification

4 Description of testability and diagnostic testing

4.1 General

The efficient and cost effective operation and maintenance of products is aided by ensuring that testability is considered during design and also during all the phases of the life cycle. Applicable diagnostic testing methods are then incorporated into the product as a component of the maintenance concept. Implementation of testability and diagnostic testing is accomplished throughout the life cycle of a product.

Life cycle cost (LCC) is an increasingly important aspect in evaluating the quality of any design. In addition to the immediate acquisition cost, many customers demand control of the costs associated with day to day operation, maintenance and logistic support. These costs are primarily influenced by the product's reliability, maintainability and maintenance support characteristics. In this context, the application of diagnostic testing techniques can be a significant contributory factor in the reduction of certain cost elements in the LCC. Constraints resulting from LCC optimization efforts should therefore be taken into account whenever diagnostic testing requirements are established.

This International Standard is intended to be applicable to all phases of the life cycle, i.e. from the time when the need for a product is identified through the design and development phase, to the manufacturing and installation phase and finally to the operation and maintenance phase as follows (see also Figure 1).

a) **Design and development phase**
From the concept down to the realization of a product, the requirements placed on a

product should be adapted to the specific needs of its field of application, where necessary passing through several pre-phases.

b) **Manufacturing and installation phase**
During this phase, it may be necessary to verify the diagnostic techniques using actual equipment and assess the product's effectiveness. Documentation can be prepared and training can now occur for operational and maintenance personnel.

c) **Operation and maintenance phase**
There may be a change to tested equipment due to obsolescence. The testing function may need to be continued and replacement or upgrading of equipment should take into account a continuing need for diagnostic testing. In the latter case, a redesign should be carried out in a new development phase.

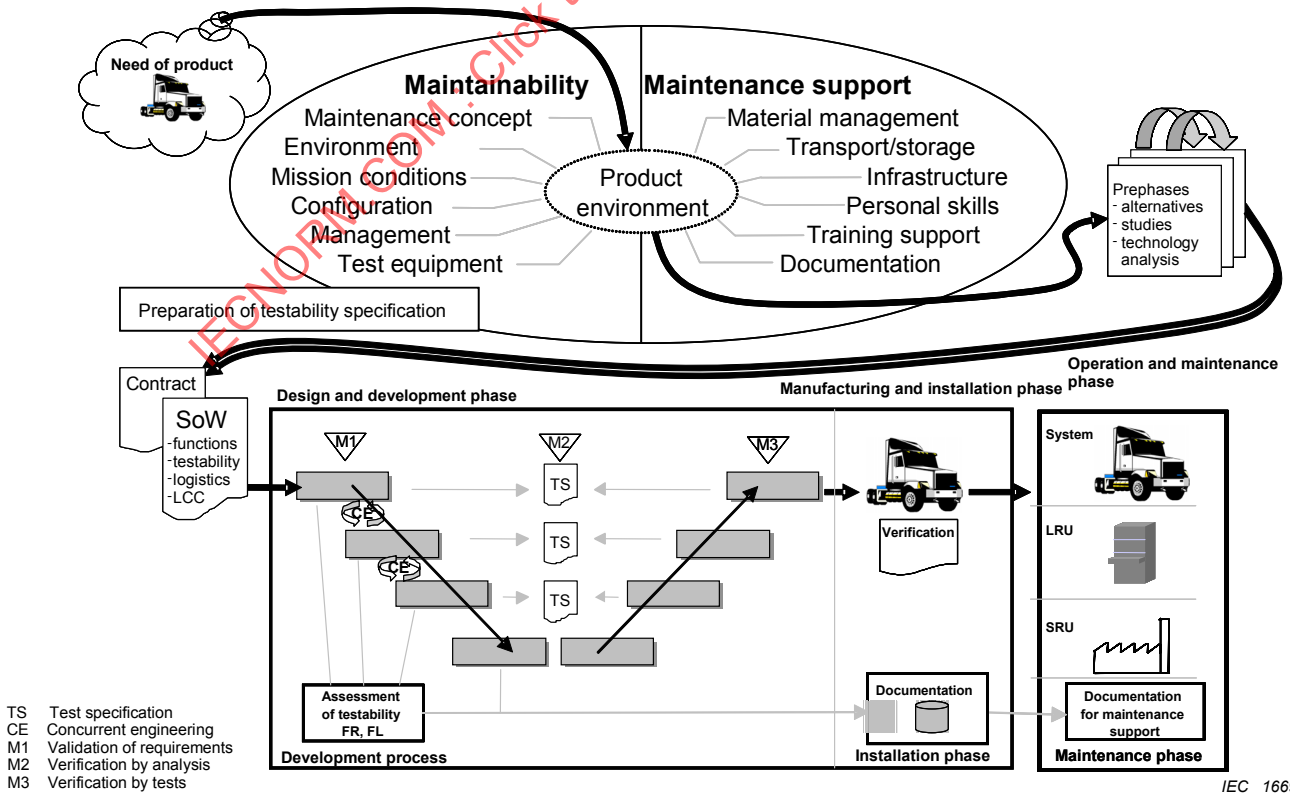
By applying this International Standard, the preconditions are assumed to be fulfilled for generating the necessary product data/information and that this can be verified and updated over the product's complete life cycle.

Annex B gives an example of how testability is developed, documented and verified with regard to product/system design.

Diagnostic testing can consist of

– functional testing with the purpose of verifying that a function can still be performed;
– condition monitoring which is intended to track the condition of equipment that degrades over time.

Condition monitoring is closely related to the concepts covered by diagnostic testing, and cannot, and should not, be dissociated from it. However, it is not the intention that full coverage of condition monitoring should be part of this standard.



TS Test specification
CE Concurrent engineering
M1 Validation of requirements
M2 Verification by analysis
M3 Verification by tests

IEC 1669/07

Figure 1 – Testability and diagnostic testing during the life cycle

4.2 Objectives of testability

Testability during design and development is closely aligned with maintainability, availability and safety and the main objective of testability is to address the following questions for each of the system functions.

a) Can the function's failures be detected by a diagnostic test ? Certain functions cannot be completely tested because of safety constraints or because the test may be destructive (such as testing the overspeed mechanism on a rotor).

b) Is it practical to test? The criticality of the function's failure, the test costs (the test equipment cost, the test equipment maintenance costs as well as the test activity costs) and the use of better and cheaper alternatives may result in the conclusion that it is not cost effective to test.

NOTE For both the cases in a) and b), alternative methods should be adopted to ensure the performance of these functions is maintained during the life of the product. Together, these elements contribute to the test coverage. A low test coverage value may be detrimental in that the system cannot be tested to confirm operational performance during its life cycle, but it may also indicate that the maintainability and maintenance capability is such that testing is not necessary.

c) In what stages in the life cycle should the item be tested? The ability to test should be considered for each stage in the life cycle; testing a function at unit level may be possible, but impractical at system level. This can best be explained by an example: consider a washing machine and its function to discharge waste water. It would be useful, from a user perspective, to run a pre-operation stage test to confirm that the function can be performed prior to operation (running an operational stage test would provide little benefit). The design for this function may not require the introduction of test equipment to test this function because

   1) the life of the pump and associated equipment well exceeds the life of the product (other failures and the expense of their repair may define the product's life);

   2) the maintenance task to remove a possible blockage can be easily accommodated;

   3) units that perform this function can be fully tested at the unit stage and at the system level stage prior to delivery;

   4) determining the stages to test can also influence the life cycle cost;

d) To what depth should it be tested? The depth of test is also an important criterion and, as in the above example, it is closely aligned to the maintenance concept. The depth of test specifies the level to which the unit or sub-unit is to be identified. For example, a system test may identify the unit to be replaced, but can also identify the sub-unit that needs to be replaced with little or no impact on the cost. This may reduce the costs associated with the test equipment required at the unit level to identify and replace the faulty sub-unit.

   It is a basic principle in the design of testability that all functions developed should be verifiable. It should, however, be noted that test coverage of 100 % is not necessarily desirable, as testing can create failures that manifest themselves during operation, which may be worse than not testing, e.g. real failures introduced by testing or false alarms. Nor is test coverage of 100 % recommended for all safety issues, as the test itself may prejudice the safety of the system. It is more important that tests give substantial confidence in the operation of the system. To achieve this, deviations from test coverage of 100 % should always be thoroughly substantiated.

   Nevertheless, the objectives of testability should not contradict higher ranking objectives, e.g. availability.

e) How should false alarms and no fault found be managed? The system test may detect and report a failure to the user when a failure does not truly exist. This may cause unnecessary investigations and result in the report of a false alarm. It may also generate unnecessary maintenance action that concludes in a No Fault Found diagnosis. False alarm rates for the various resolutions should not exceed the defined criteria and, where possible, be reduced to zero. Methods that are recognised to minimise these occurrences may involve feedback systems that constantly assess the environment and recalibrate themselves to allow for component degradation within the defined criteria. Repeating a test to eliminate a false alarm (the scenario of the test may have changed sufficiently for the alarm not to be generated) will increase the test time and should be avoided.

   Faults can be indicated where no faults exist. This can be due to a number of reasons:

   1) if a fault found in the system and the diagnostic identifies the faulty item, but upon removal of the item and testing the item independently no fault can be identified, then you have to check the test specification from the system in relation to the test specification from the faulty item;
   2) poor diagnostics (the test does not adequately identify the faulty part);
   3) interface difficulties (for example, a connector fault may have resulted in a unit being removed and a re-connection removes the failure);
   4) poor test equipment including BITE (for example, a detected failure that does not exist);
   5) intermittent fault (rogue units can sometimes contain faults that are not evident except in certain circumstances);
   6) design tolerance tiering problems (a failure at system test may not register failure at unit test). Rogue units can have extreme values in the tolerance band that results in continual rejection;
   7) software faults (faults appearing during usage that are not suitably tested);
   8) maintainer and user difficulties (inadequate training, speed of turn around, lack of spares) can all result in good units being rejected.

   All the above symptoms can have an adverse affect upon operations and support and should be eliminated or minimised wherever possible;

f) Can system testing be tailored? System testing is concerned with providing assurance that a system will function correctly given defined inputs and within a defined environment. The testability requirements and ability to localise a fault does not necessarily dictate the test procedure. Testing an overall function, with subsequent deeper testing if necessary, can provide substantial timesaving and greatly improve user friendliness. Use of tools such as FMECA (see Annex B) and FTA can assist in defining the sequence of lower level testing by determining the most probable sub-function to have failed.

4.3 Objectives of diagnostic testing

The objective of diagnostic testing is to provide the most cost effective, rapid and unambiguous method of fault identification to a level determined by the maintenance concept for the equipment under test. Good diagnostic testing will

- increase equipment availability;
- decrease maintenance costs;
- reduce the risk of consequential damage;

- improve the safety of the system;
- optimize the operational use.

To achieve the objective, the diagnostic system should

- provide confidence type checks to confirm the serviceability of the equipment for its intended role;
- recognize catastrophic and degradation failures;
- localize faults with respect to the failed function or LRU;
- warn of impending wear-out failures, by evaluation of wear-out states;
- provide data for operation and maintenance of the equipment.

The principal applications of diagnostic testing facilities are

- safety and functional checks prior to the operation of the system;
- performance monitoring during operation;
- equipment failure identification in the operating environment to failed assembly or LRU level;
- detailed fault localization in the designated repair facility.

4.4 Methods used for diagnostic testing

The possible procedures which can be applied for diagnostic testing range from purely manual measurements and evaluation of mechanical characteristics to fully automated diagnosis of entire processes and installations, with the testing of single components and complex systems. The broad diagnostic methods applied fall into two main categories:

– external diagnosis that utilizes test equipment discrete from the product which is only connected when required. The test equipment used may be of a general purpose nature, adapted for the purpose from standard or specially designed for the equipment to be tested. Computer controlled ATE may also be involved;

– internal diagnosis that utilizes permanently built-in test equipment (BITE) which may be continuously or intermittently operated during the operation of the system. In addition, special tests, in the reduced, or non-operating state of the system, may also be performed.

4.5 Methods used for condition monitoring

In addition to diagnostic testing which tests for discrete faults, many products also benefit from condition monitoring. This is performed as a part of preventive maintenance to monitor degradation of condition and performance.

Methods used for condition monitoring will vary with the type of equipment and may include

– vibration analysis;

– fluid/lubricant analysis;

– ultrasonic detection;

– thermography;

– alarms and shutdowns built into the control system.

4.6 Concept of testability

Testability is the design characteristic of a product which guarantees that the functional capability of that unit can be assessed in a timely and efficient manner and that faults can be recognized and, where necessary, localized. It is a primary component of ensuring the maintainability of a product.

Diagnostic testing is the resultant maintenance action that occurs as a part of preventive maintenance as described in the maintenance concept. Test coverage is the degree to which diagnostic testing can be applied. Diagnostic testing consists of two steps: fault recognition (FR) and fault localization (FL). Fault recognition identifies whether a fault exists and fault localization determines the specific nature of the fault.

Diagnostic testing should also consider tolerance chains. For a particular parameter, there is usually an upper limit and a lower limit that bounds the pass and fail regions. A unit function may have tight limits, but as the unit is integrated, these limits are affected by the variability of other units that contribute to the final system function. In addition to the tolerance chains, the accuracy of the test equipment undertaking the test should be considered before the actual pass/fail tolerance band can be defined for a particular test. The test results gathered during development provide an estimation of the process width (the summation of the function production yield and the accuracy of the test equipment, including the accuracy of the test equipment stimuli as well as the reading accuracy of the measuring device). It is not the intention that full coverage of tolerance chains should be part of this standard.

The specifications relating to functionality, including testability, in the form of the characteristic value for the quality of the fault recognition and fault localization have a direct impact on the basic functional features of the product. If the rule "functions that are to be developed should be verifiable via parameters" is followed, then FR and FL are developed concurrently from the very beginning as an integral part of the functionality. In this way, the cost of a product will remain within the prescribed limits. If elements of the FR and FL are integrated at a later date, this will lead not only to considerable delays but also to a reduced product quality with extremely high costs of rework/corrective action.

5 Testability specification

5.1 General

Appropriate contractual provisions are a key prerequisite for efficient conversion of diagnostic testing requirements into measurable practical achievements. In order to enable optimum design, development and supply of diagnostic test procedures, the customer should provide a detailed specification of testability requirements and constraints. For this purpose, the customer should provide the supplier with the following documents:

– a statement of work (SoW). This document contains all the functional requirements related to testing. Within this document, the customer specifies all of the expected functions/functionalities, including testability;

– a testability specification. In this document the contractor (developer) determines the means (hardware, software) to realize the operational and test engineering functions and performance features required by the SoW.

5.2 Statement of work

The SoW contains detailed descriptions of the customer's needs and is intended to form the basis of the design and development programme. Updating is possible, if additional information becomes available in the course of development. However, modifications should be mutually agreed upon, as they will often incur additional time and cost penalties. The requirements should include

– objectives of diagnostic testing (see 4.3);
– operational concept (see 5.3 and Table 1);
– maintenance concept (see 5.3 and Table 2);
– qualitative description of the economical environment (see 4.1);
– preferred methods and solutions (see 4.4).

5.3 Specification

The testability specification determines the testability requirements for the product and possibly for the development phase. The testability specification should define each of the test stages and the associated function elements for which the test specification is applicable. These should include the following.

a) Tasks and applications of diagnostic testing should include:
   1) a list of safety faults for which a fault recognition of as close to 100 % as possible is required;
   2) a list of critical faults for which a test coverage of 100 % is required or supporting evidence to justify why the test can be omitted;
   3) a lower limit of test coverage for all other functions or global test coverage for all functions (functions to be used for test coverage have to be determined);
   4) a maximum value of the fault recognition time;
   5) target (maximum) values of the fault localization time;
   6) a target and minimum value of the diagnosis correctness;
   7) a maximum value of the false alarm rate.
b) Design for testability should include:
   1) general requirements;
   2) detailed requirements by checklists;
   3) design criteria for testability.
c) Times and procedures for the following:
   1) testability verification;
   2) safety verification.

The consequences of not meeting the specified requirements according to the above elements should be defined in advance.

Test tasks that should be specified are further described in 5.4.3. The need for evaluation of alternative methods (see 5.6) should be identified at this stage.

Diagnostic testing activities are closely interconnected with the processes of the product's operation and maintenance. Therefore, the operational and maintenance concepts are important factors to be considered when diagnostic testing requirements are established. They should both be defined as early as possible in the system life cycle, preferably in the concept and definition phase. The operational concept should be the first consideration in order for the system to properly fulfill its requirement. The maintenance concept should be designed to allow the operational need to be met with the most efficient use of resources at minimum cost. A

degree of trade-off will invariably have to be considered to achieve the optimum balance of what can often be conflicting requirements.

The elements that should be considered in defining the operational concept are given in Table 1. Each element should be specified in detail in order that the maintenance environment and the operational constraints can be properly considered.

The maintenance concept determines the test tasks to be applied at the correct design level, the personnel to carry them out and the test equipment to be used. The needs of all those involved in the product (development, production, operation and maintenance) should be taken into account. Table 2 contains a list of elements of the maintenance concept to be considered.

Table 1 – Elements of the operational concept

Element	Possibilities		
Location	Mobile		
	Stationary	Transportable	Varying location
			Fixed location
		Not transportable	
Operational mode	Continuous operation	Continuous monitoring	
		Monitoring at discrete points of time	
		Allowable breaks and break conditions	
	Intermittent operation, including conditions of intermittence		
Operational stress condition	Operation at partial stress		
	Operation at nominal stress		
	Operation at overstress		
Consequences	Safety		
	Cost	Reduced utilization	
		Consequential damage	
		Maintenance costs	
	Corrective, emergency measures		
Environmental conditions	Mechanical stress		
	Thermal stress		
	Electrical stress		
	Chemical stress		
	Others		
Personnel	Untrained		
	Trained in different area		
	Trained	High qualification	
		Medium qualification	
		Low qualification	
Handling	Manual		
	Partially automated		
	Fully automated		

Table 2 – Elements of the maintenance concept

Element	Required details		
Maintenance tasks	Preventive	Maintenance	
		Diagnostic test	
		Scheduled repair	
	Corrective	System level	Fault recognition
			Fault localization
			Repair (replacement)
			Calibration
			Functional check
		Component level	Fault localization
			Repair
			Calibration
			Functional test
Maintenance time	Continuous monitoring		
	Preventive maintenance	Intervals	Time period
			Action
		Type	Level
			Hard time maintenance
			On condition maintenance
	Corrective maintenance		
Maintenance location	Stationary	Number of shops	
		Local distribution of shops	
		Technical potential of shops	
	Mobile	Equipment of station	
		Technical potential of station	
Maintenance procedure	Procedure		
	Resources	Hardware	
		Software	
	Documentation (descriptive, illustrative) for		Hardware
			Software
Maintenance support	Stock	Number of stores	
		Local distribution of stores	
		Stock size	
		Storage conditions	
	Stock management	Procurement	
		Supply	
		Transportation	
Maintenance environment	Thermal conditions		
	Other conditions		
Maintenance personnel	Basic training	Branch of training	
		Qualification level	
	Special training	System level	
		Component level	
	Refresher training	Intervals	
		Curricula	

5.4 Characteristics of testability

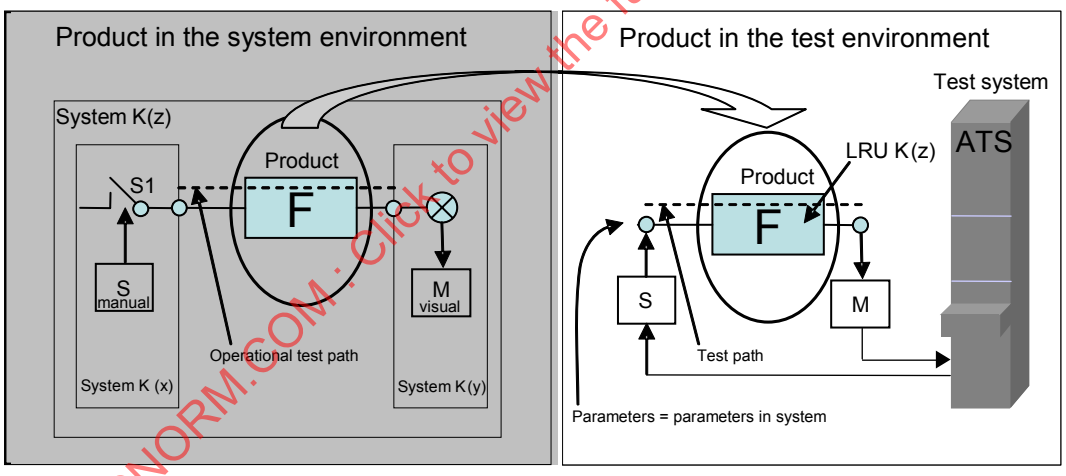
5.4.1 Testability features

The testability features can be characterized by the following parameters (mathematical expressions are given in Annex A):

– fault recognition: see IEC 60050-191;
– fault recognition time: see 3.1.11;
– fault localization: see IEC 60050-191;
– fault localization time: see IEC 60050-191;
– diagnosis correctness: see 3.1.7;
– test coverage: see 3.1.33;
– false alarm rate: see 3.1.10.

5.4.2 Operational context

A product can be used in different environments, depending on the requirements that are placed on that product in the SoW. As far as testability is concerned, a distinction is made between the system environment (operating condition) at the stipulated design level as shown in Figure 2 and the test environment corresponding to the required maintenance conditions. In the latter, the product is operated in a system/product simulation. Here, all the parameters set for testing the hardware unit should correspond to those in the system. Figure 2 shows how the one relates to the other.



Key

S Stimulus
M Measurement
F Function
K(x),K(y),K(z) Systems (items) being part of the breakdown structure

IEC 1670/07

Figure 2 – Operational context

5.4.3 Test tasks

5.4.3.1 Test paths

The smallest unit of a test comprises a test path that starts with at least one stimulus, passes via a function/sub-function and ends with the minimum of one measurement including a comparison with the specified value.

Test paths required for fault recognition pass through any functions of a chain of replaceable units.

Test paths required for fault localization should consist of tests on physical interfaces between replaceable units.

The test task comprises fault recognition and localization and is conducted in the portions A + B + C + D = 100 % as shown in Table 3.

Table 3 – Test task

Portion	Test tasks	Example specified values *FR*	Example specified values *FL*
A	Tests during operation (on-line test)	50 %	0 %
B	Tests under test conditions, without external test equipment (off-line test)	50 %	95 %
C	Test under test conditions, with external test equipment	0 %	5 %
D	Not testable	0 %	0 %

All tests listed in Table 3 are available for fault localization. The localization of defective replaceable hardware units (LRUs/SRUs) is achieved from information contained in the test results obtained from the series of tests that cover different test paths crossing through the LRU/SRU. The functional model (see Annex B) provides the information needed. In this example, there is only test coverage for *FR* in portions A and B and *FL* in portions B and C.

The product design should provide features enabling all test tasks to be carried out in accordance with the requirements set out in the SoW. These features are sub-divided into the test feature BIT and, where allowed, external test equipment with the necessary test inputs.

5.4.3.2 Built-in test

BIT is a feature of the product for the purpose of performing tests. A BIT function consists of at least one stimulus, a test path via one function/sub-function and at least one measurement including comparison with the specified value. The number of BIT functions required is derived from the requirements given in the SoW and depends on the specified values laid down for fault recognition. BIT consists of hardware and software portions.

NOTE In electronic equipment, failure detection may often be achieved by simply monitoring certain vital parameters, for example supply voltages, power shape or frequency of well-defined signals, identities of discrete signals or checksums of data. These are specialized forms of on-line BIT where no extra stimuli are applied. Instead, through BITE, additional reference signals are generated to allow the BIT to compare them with the required values.

BIT tests form part of all the functional tests conducted on a product and are divided into on-line and off-line tests.

On-line tests are those that are conducted continuously while a product is in operation.

Operation has to be interrupted before off-line tests can be carried out. Such tests should generally only be used for fault localization purposes.

5.4.3.3 Testing by means of external test equipment

If external test equipment is needed and is allowed by the SoW, then the product is accessed via test inputs (e.g. test connectors). External test equipment works on the same principle as BIT functions and therefore requires test paths from the stimuli, via the function to be tested through to the measurement point, with inclusion of the assessment of the test result.

5.5 Characteristic values for assessing testability

To achieve a uniform assessment of testability for all users of this standard, it is necessary to introduce characteristic values for components of testability (*FR*, *FL* and test coverage). These values are product-neutral, they reflect the required performance of the testable product and are comparable for all users of this standard.

The characteristic values should be specified in advance in the SoW. They are the point of reference for the assessment of testability. When specifying the characteristic values, the maintenance concept, the engineering effort and the associated costs should also be taken into account. If the requirements are already available to the development engineer, then he should assess the testability verification and safety verification.

The consequences of not meeting the specified requirements according to the above elements should be defined in advance.

5.6 Criteria for evaluation of alternative diagnostic designs

The possible alternative diagnostic designs should be compared and evaluated in order to select the optimum solution. The following economic criteria should be taken into account.

a) Capital cost consisting of
   1) numbers of systems required based on usage and availability;
   2) development cost;
   3) nonrecurring software cost;
   4) maintenance installation cost.
b) Equipment unit cost influenced by
   1) complexity;
   2) quantity to be produced;
   3) degree of redundancy;
   4) degree of BIT capability;
   5) quality standard.
c) Maintenance related cost consisting of
   1) preventive and corrective maintenance cost;
   2) savings by diagnostic system preventing consequential damage;
   3) degree of automation considered against training levels;
   4) planned equipment life.
d) Means to increase operating profit such as
   1) improved handling characteristics;
   2) increased availability e.g. by quick diagnosis and repair of faults or by use of redundancy;
   3) increased utilization.
e) Other factors including
   1) modification potential;
   2) technical and cost impact of additional hardware or software on safety and reliability of equipment;

3) capability to recognize transient and intermittent failures;
4) revert mode capability of diagnostic system;
5) cost efficiency gains using BITE compared with external test equipment;
6) use of COTS.

6 Testability in the development process

6.1 General

Once all the requirements from the sphere of operation of the product have been worked out, then the product development can be started.

The successful development of a product is primarily based on uniformly defined instructions on how to proceed. This provides a common understanding of the requirements relating to the development, updating and modification of a product to all parties involved. This applies equally to accompanying activities such as quality assurance, configuration management and technical project management.

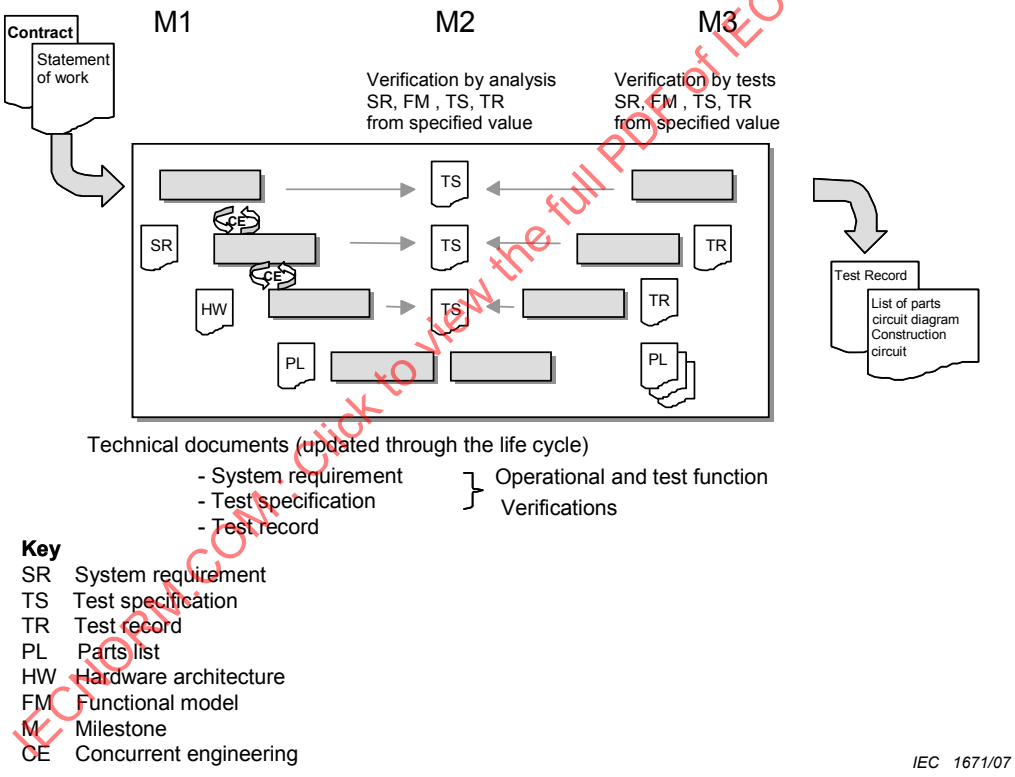


Figure 3 – Development process in the V-model

Three milestones should be prescribed when developing testable products:

– M1 – start of development by the contractor with the validation of the requirements;
– M2 – theoretical proof of the product's testability with the verification by analysis;
– M3 – practical demonstration of the product's testability with the verification by tests.

Figure 3 shows how these are linked to the development process in a V-shape model.

The following steps are necessary in order to arrive at a testable product:

– check requirements for completeness and, where necessary, request that the customer provides any missing requirements;
– carry out a requirements analysis to generate a specification;
– assign the product to the design levels prescribed by the customer;
– carry out functional design (functions/sub-functions and link them);
– carry out engineering design (hardware assignment);
– develop fault recognition and optimize where necessary;
– develop fault localization and optimize where necessary;
– prepare verification activities;
– carry out verification;
– document verification.

As soon as the hardware units have been defined in the development project, these units trigger a new process at a deeper design level in accordance with the prescribed description of tasks. If certain functionalities cannot be realized by way of the defined hardware unit, then an iterative improvement process is started by which modified specifications are worked out at the previous level and then a new hardware unit is defined. Once all the hardware units have been defined down to the individual components, then the integration process can be started in the description of tasks.

The application of standards and associated computerized tools facilitates development considerably.

6.2 Functional assignment

The testability development process is based on the requirement that all functions and sub-functions contained in the product should be verifiable. This is achieved by adequate allocation of test steps to hardware units and associated sub-functions.

An appropriate procedure for the implementation of the testability requirement is described in Annex B. It is a type of FMEA method based only on a functional model.

6.3 Testability engineering

6.3.1 Design criteria for testability

The purpose of this programme element is to provide the means of achieving the diagnostic testing requirements established for the product. This is part of maintainability during the design, which is covered in IEC 60300-3-10 and IEC 60706-2. In this context, the following testability design criteria should be considered:

– functional partitioning into functional groups and units with clearly-arranged and well-defined interfaces. Whenever possible, the physical and electrical partitioning should be compatible with this structure in order to facilitate optimum adjustment of diagnostics, maintenance and logistics;
– preference for the use of functions, components and design elements, the status and the transitional behaviour of which can be measured and evaluated easily by simple and appropriate diagnostic test procedures;
– consideration of those measuring procedures that are applicable during maintenance and compatible with existing or planned external equipment. The physical and electrical accessibility of the measuring equipment should also be taken into account;
– the extent of self-testing should be consistent with level of repair analysis (LORA) as described in IEC 60300-3-10;
– test points should be provided and appropriately labelled, especially those required for external test equipment;

– failure definitions and scoring criteria should be well defined prior to finalizing the product's testability criteria;

– initialization: the system or equipment should be designed such that it has a well-defined initial state to commence the fault localization process. In case of a failure, the initialization should take place automatically and repeatedly;

– application of test procedures and external stimuli should have no harmful effects on the component itself nor on related equipment or the overall system;

– all bus-systems should be accessible for measurement;

– the functional and, where applicable, diagnostic application software should be designed and documented such that it can be readily verified by the maintenance personnel.

6.3.2 Design for testability

Once the decision as to what functions are to be realized in the hardware units has been taken, these hardware units should be assigned to the product's design levels. The breakdown of these is hierarchical (top down). The number of levels depends on the complexity of the product/system and its technical design. For simplification/standardization purposes, the individual design levels from component up to system are given classifications (K1 … Kn). Higher system levels may be introduced, but only receive consecutive numbering (e.g. system 4, system 5, etc.).

In the course of engineering design, functions/sub-functions are assigned to the hardware units. Here, attention needs to be paid to the following:

a) minimum number of interfaces (where sub-functions are separated);

b) functional grouping (combination of SF with the associated higher-level function);

c) only use standardized interfaces (e.g. bus). Where necessary introduce a separate test bus.

The design for testability should incorporate the various test stages involved in the life of the system. This includes

1) the production phase;

2) the storage phase;

3) the pre-operation phase;

4) the operation phase;

5) the post-operation phase;

6) the maintenance steps; and

7) the disposal phase.

Each stage should be addressed separately and collectively to achieve a cost effective solution for the testability of a product. It should also be considered that some systems operate multi-roles and may be used in different scenarios, causing different functional elements to be exercised, and these elements should be similarly addressed.

6.3.3 Use of commercial off-the-shelf products (COTS)

A precondition for the use of COTS products is that they meet the requirements set out in the SoW and thus meet all the needs relating to the sphere of operation, including testability, maintenance and the availability of the documentation needed for the in-service phase. In the case where the commercial off-the-shelf product does not meet the requirements of testability set out in the SoW, then the development engineer should implement the missing part of testability function into the system.

Because the prime contractor may not be the COTS vendor, both parties may need to perform an evaluation through a co-operative effort. The amount of testing required is to ensure that the COTS item meets the operational and environmental requirements that are specified for the prime contractor's product. What may be needed is to require the supplier to furnish operational and environmental characterization data and the results of testing to substantiate reliability and maintainability claims. Also, it may be necessary to require that the supplier provide evidence that the manufacturing processes do not compromise the designed-in reliability and maintainability characteristics. This evidence may include the results of sampling tests or control charts showing that critical processes are in control with a high process capability.

6.4 Testability development process

6.4.1 Logistic support

The planned maintenance support of the product should be specified by the customer in the SoW so that the development engineer can determine the consequences of the assignment (e.g. higher priority for BIT functions). If the product to be developed contains replaceable standard hardware units such as lamps, fuses, filter elements, etc., then the customer should also determine the logistic assignment of these in the SoW (see Figure 4 and Table 4).

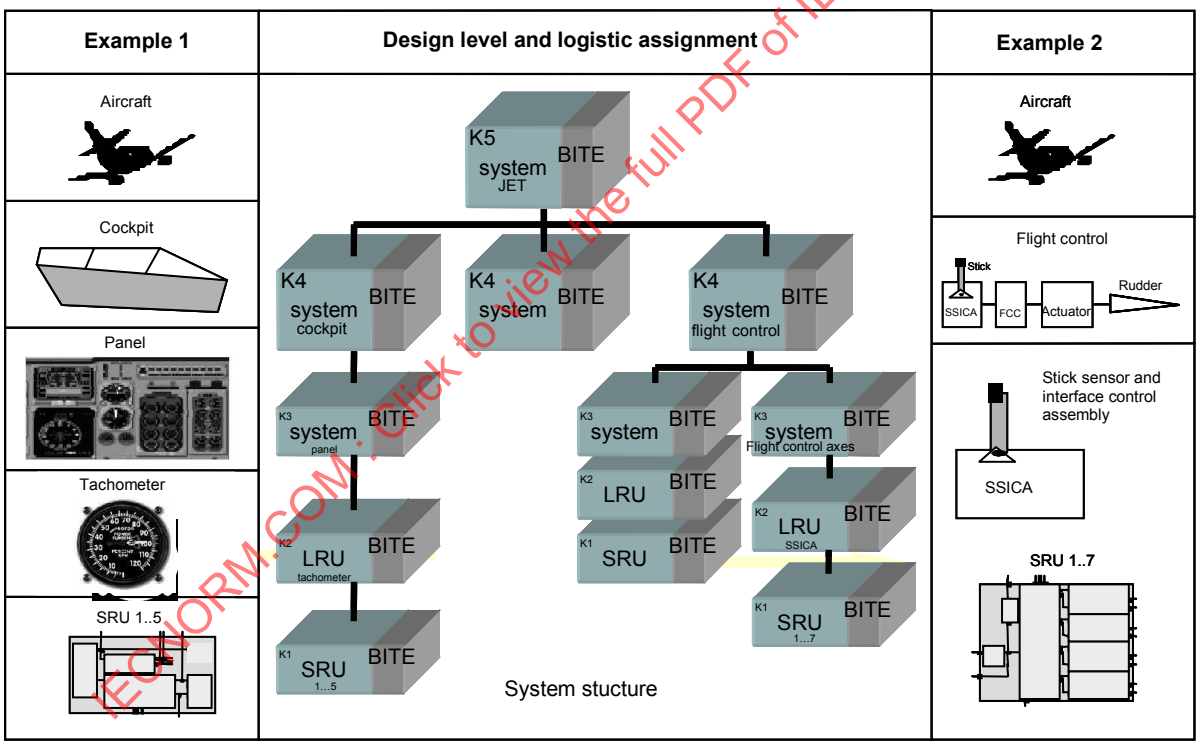


Figure 4 – Design levels and their logistic assignment, taking an aircraft as an example

Table 4 – Example of logistic assignment

Design level	Logistic assignment	Example
K5		Aircraft
K4		Cockpit, flight control system
K3		Panel 1, flight control axis
K2	LRU	Tachometer, SSICA
K1	SRU	Plug-in cards, PCBs

6.4.2 Availability and diagnostic testing

In the design and development phase, testability features and characteristics should be incorporated into the design in accordance with the results of related initial trade-off studies. Specific consideration should be given to diagnostic testing techniques having the potential to improve the product's maintainability and minimizing down time, thus increasing availability and profit and decreasing overall costs.

In the case of items with inherent wear-out characteristics, improvements primarily affect the cost of preventive maintenance, which can be significantly decreased by diagnostic test procedures, particularly where optimization of maintenance intervals and of the necessary amount of preventive maintenance work and resources can be achieved. If no wear-out is involved, as is the case for most solid state electronic systems, the cost of preventive maintenance is negligible, and the highest cost impact is caused by the capital costs, which are in turn largely dependent on the achieved availability. Since the major portion of down time is the fault recognition and localization times, emphasis on diagnostics is most effectively placed on these elements.

7 Assessment of testability

7.1 General

The purpose of the verification programme is to prove, initially by theoretical and later by practical means, that the diagnostic testing requirements have been fulfilled. This can be done by methods and procedures similar to those applied for the verification of maintainability parameters (see IEC 60706-3). Verification concepts that should be considered include

– verification by analysis;
– verification by tests.

7.2 Verification by analysis

Elements of the verification by analysis are as follows:

– documentation review: documents supplied in response to the requirements in 5 should be reviewed with respect to completeness, accuracy and ease of use;
– analysis: this activity includes the analytical investigation of the item and the assessment of its testability features in accordance with Annex B.

7.3 Verification by tests

Verification by tests is carried out on the product hardware. If this is required in the SoW, then it should be carried out during acceptance of the development result and the test specification provides the basis for this verification. Fault simulation is effected through non-destructive interventions in the hardware units and/or, where necessary, simulation via software, but this should be supported by practical evidence. For non-testable functions, evidence must be provided to substantiate the suitability of the design.

Further information on verification of testability is given in Annex B.

8 Testability documentation

It is important to ensure that full documentation of the diagnostic concept is supplied in a standardized form, so that all the relevant information is made available to the operators and maintainers of the system. The design of the documentation should take into account the operational context for both usage and maintenance, the maintenance concept, levels of skill, and degree of training to be given. Further details on testability documentation are given in Annex B.

Annex A
(informative)

Calculation of characteristics of fault recognition and fault localization

A.1 Symbols

m number of hardware units

n number of terminals

h fault recognition during operation

k fault recognition under test conditions

l fault localization at terminal

*v*1 fault localization on one hardware unit

*v*2 fault localization on one of two hardware units

*v*3 fault localization on one of three hardware units

A portion of tests during operation (on-line tests)

B portion of tests under test conditions without external test equipment

C portion of tests under test conditions with external test equipment (ext. tests)

D portion of preventive maintenance (maintenance tests)

A.2 Fault recognition during operation

The symbol h_i means that a fault can be recognized at terminal *i* during operation.

h_i = 1: fault recognition at terminal *i* during operation;

h_i = 0: no fault recognition at terminal *i* during operation;

$\sum_{i=1}^{n} h_i$ = number of terminals where a fault can be recognized during operation.

Thus, the characteristic for fault recognition during operation is as follows:

$$FR_{(A)} = \frac{\sum_{i=1}^{n} h_i}{n} \times 100\ [\%]$$

A.3 Fault recognition under test conditions

The symbol k_i means that a fault can be recognized at terminal i under test conditions.

k_i = 1: fault recognition at terminal i under test conditions;

k_i = 0: no fault recognition at terminal i under test conditions;

$\sum_{i=1}^{n} k_i$ = number of terminals where a fault can be recognized under test conditions.

Thus, the characteristic for fault recognition under test conditions is

$$FR_{(A+B+C+D)} = \frac{\sum_{i=1}^{n} k_i}{n} \times 100\ [\%]$$

Note on the optimization of test paths being part of test portion A (on-line tests).

Due to cost efficiency it may be useful to optimize the number of necessary test paths for fault recognition during on-line tests with respect to the failure rate (λ) of a sub-function.

FR = fault recognition (portion A) depending on the failure rate of the sub-function

SF = sub-function

P_{SFi} = number of testable ports of sub-function i

ΣP_{SFi} = sum of all ports of sub-function i

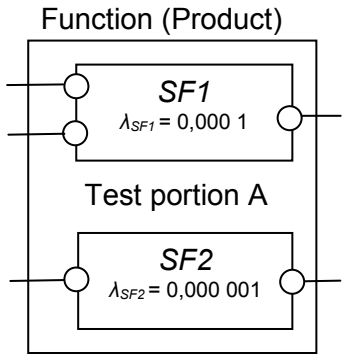
λ_{SFi} = failure rate of sub-function i

$\Sigma \lambda_{SFi}$ = sum of all failure rates of sub-functions i

Formula:

$$FR = \sum_{i=1}^{n} \frac{P_{SFi}}{\sum P_{SFi}} * \frac{\lambda_{SFi}}{\sum \lambda_{SFi}} \leq 1$$

Example:



P_{SF1} = 3 λ_{SF1} = 0,0001

$\sum P_{SF1}$ = 3 λ_{SF2} = 0,000001

P_{SF2} = 2 $\sum \lambda_{SF}$ = 0,000101

$\sum P_{SF2}$ = 2

$$FR = (\frac{3}{3}) * (\frac{0{,}0001}{0{,}000101}) + (\frac{2}{2}) * (\frac{0{,}000001}{0{,}000101}) \leq 1$$

$$FR = (1) * (0{,}99) + (1) * (0{,}0099) \leq 1$$

$$FR = (0{,}99) * 100\% + (0{,}0099) * 100\% \leq 100\%$$

$$FR = (SF1)99\% + (SF2)1\% = 100\%$$

Result:

The probability that sub-function *SF2* will fail is about 1%. For this reason testing this sub-function may be transferred to test portions B or C thus minimizing the test effort for on-line tests in test portion A.

Fault localization

The symbol l_i means that a fault can be localized at terminal *i*.

l_i = 1: fault localization at terminal *i*;

l_i = 0: no fault localization at terminal *i*;

$\sum_{i=1}^{n} l_i$ = number of terminals where a fault can be localized.

Thus, the characteristic for fault localization at terminal is

$$FL = \frac{\sum_{i=1}^{n} l_i}{n} \times 100\ [\%]$$

The symbol $v1_j$ means that a fault can be unambiguously localized on hardware unit *j*.

$v1_j$ = 1: unambiguous fault localization on hardware unit *j*;

$v1_j$ = 0: no unambiguous fault localization on hardware unit *j*;

$\sum_{j=1}^{m} v1_j$ = number of hardware units where a fault can be unambiguously localized.

Thus, the characteristic for fault localization on one hardware unit is

$$FL_{v1} = \frac{\sum_{j=1}^{m} v1_j}{m} \times 100\ [\%]$$

The symbol $v2_j$ means that a fault can be localized on one of two hardware units, one of which is unit *j*.

$v2_j$ = 1: fault localization on hardware unit *j* or one other hardware unit;

$v2_j$ = 0: no fault localization on hardware unit *j* or one other hardware unit;

$\sum_{j=1}^{m} v2_j$ = number of cases where a fault can be localized on one of two hardware units.

Thus, the characteristic for fault localization on one of two hardware units is as follows:

$$FL_{v2} = \frac{\sum_{j=1}^{m} v2_j}{m} \times 100\ [\%]$$

A.4 Diagnosis correctness and test coverage

A.4.1 Symbols

Using the notation of 5.4.3.1, the following symbols are established. Values A, B, C, D are the limiting values of subsets A', A'', B', B'' C', C'', D' and D''.

A	Tests during operation (on-line tests)	
A'	On-line tests leading to a correct diagnosis	(lim A' = A)
A''	On-line tests actually provided for	(lim A'' = A)
B	Tests under test conditions without external test equipment	(off-line tests)
B'	Off-line tests leading to a correct diagnosis	(lim B' = B)
B''	Off-line tests actually provided for	(lim B'' = B)
C	Tests under test conditions with external test equipment	(ext. tests)
C'	External tests leading to a correct diagnosis	(lim C' = C)
C''	External tests actually provided for	(lim C'' = C)
D	Preventive maintenance (maintenance tests)	
D'	Maintenance tests leading to a correct diagnosis	(lim D' = D)
D''	Maintenance tests actually provided for	(lim D'' = D)

where A is the limiting value of lim A'.

A.4.2 Diagnosis correctness

According to the basic principle of testability design, it should be that

A + B + C + D = 100 %

(see 5.4.3.1), i.e. all possible faults are diagnosed in either one of the portions A, B, C, D of the test task. The diagnosis is correct in sub-quantity

A' + B' + C' + D' ≤ 100 %

Thus, diagnosis correctness D_c can be expressed by the ratio

$$D_c = \frac{A'+B'+C'+D'}{A+B+C+D} \leq 1$$

A.4.3 Test coverage

Faults which are actually covered by either one of the portions A, B, C, D of the test task are contained in sub-quantity

A'' + B'' + C'' + D'' ≤ 100 %

Thus, test coverage T_c can be expressed by the ratio

$$T_c = \frac{A''+B''+C''+D''}{A+B+C+D} \leq 1$$

Annex B
(informative)

Development process for testable products

B.1 Requirements analysis

B.1.1 Analysing the requirements of the Statement of Work

Using the guidelines given in this standard, the requirements contained in the SoW are to be analysed to establish that they are complete and unambiguous.

Formulated requirements that are not clear should be clarified by consulting the customer and reformulating these precisely in the SoW.

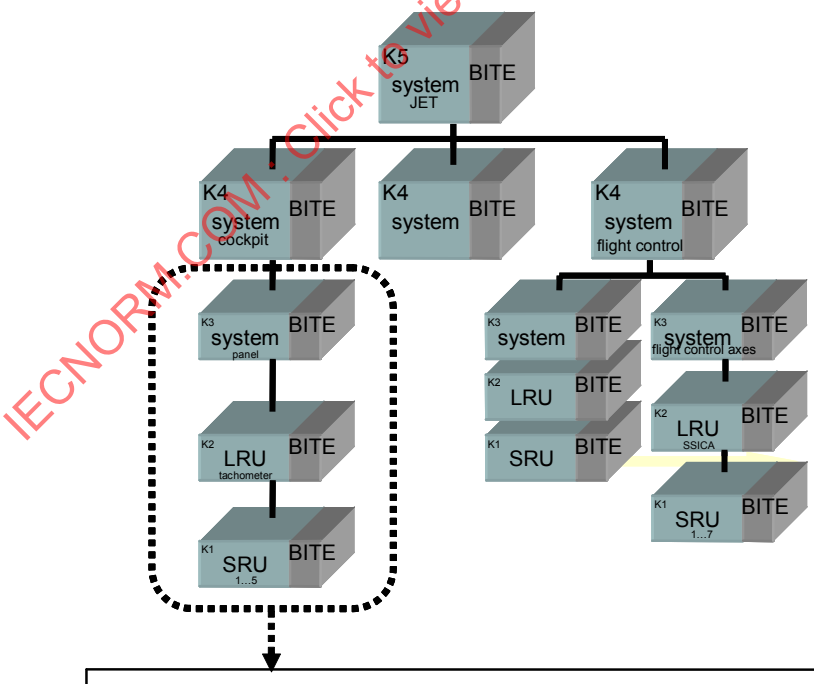
Once the SoW has been harmonized and accepted by the customer and contractor, the contract is concluded on that basis.

B.1.2 Categorization of the product to be developed

The basic data of the product to be developed (designation, item number, version, design level) are determined on the basis of the accepted SoW (see Figure B.1).

The design level to be developed is to be derived from the requirements of the SoW (e.g. design level K4).

The logistic designations (LRU/SRU) for the replaceable hardware units are to be adopted from the SoW.



Basic product data		
Designation: sample	Item number: 12345678	Version: 01
Design level: K3 system		

IEC 1673/07

Figure B.1 – Example of how to determine the basic data

The basic data have thus been determined.

B.2 Functional design

B.2.1 Listing the functions and sub-functions

At the start of development, a functional breakdown of the product in line with the required functionality is effected on the basis of the accepted SoW.

A list is made of the functions that are to be derived from the SoW.

These functions are broken down into independent sub-functions that are to be realized within the level being dealt with (see Table B.1).

Rule**:** Make a list of all the sub-functions SF that are to be developed.

Table B.1 – Data for the document “system specification"

Designation: Sample **Item number: 12345678** **Version: 01** **Design level: K3 system**	
Function	**Sub-function**
Function 1	SF1.1
	SF1.2
	SF1.3
	SF1.4
	SF1.5
Function 2	Not dealt with in example
Function 3	Not dealt with in example

B.2.2 Modelling of functions and terminals

The data for the document "system specification" are used for the modelling of the product's sub-functions and terminals (see Figure B.2).

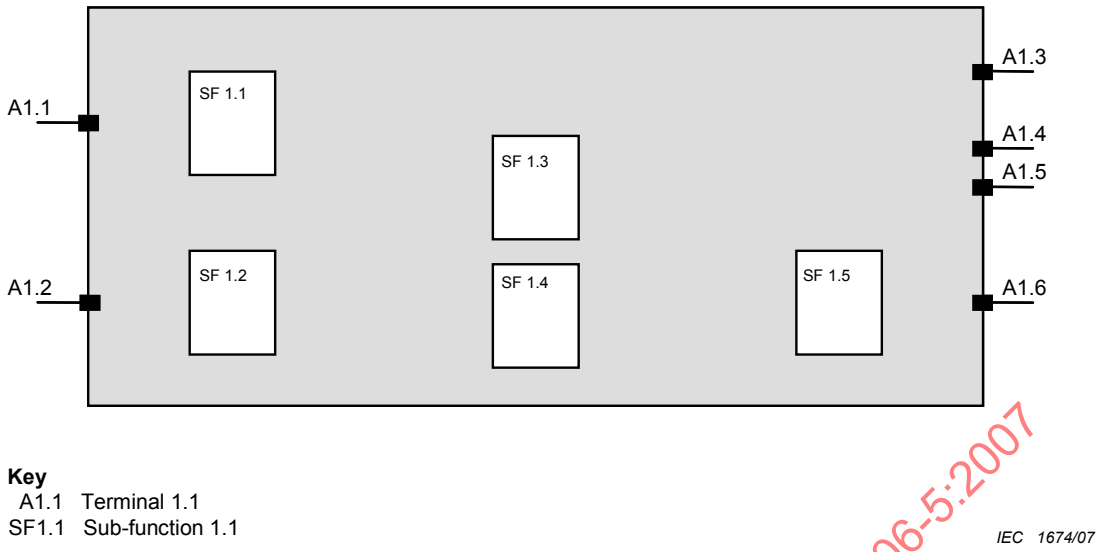


Figure B.2 – Modelling of sub-functions and terminals

A precise definition of the functional model is made. To achieve this, the determined sub-functions are interconnected by stating the functional links.

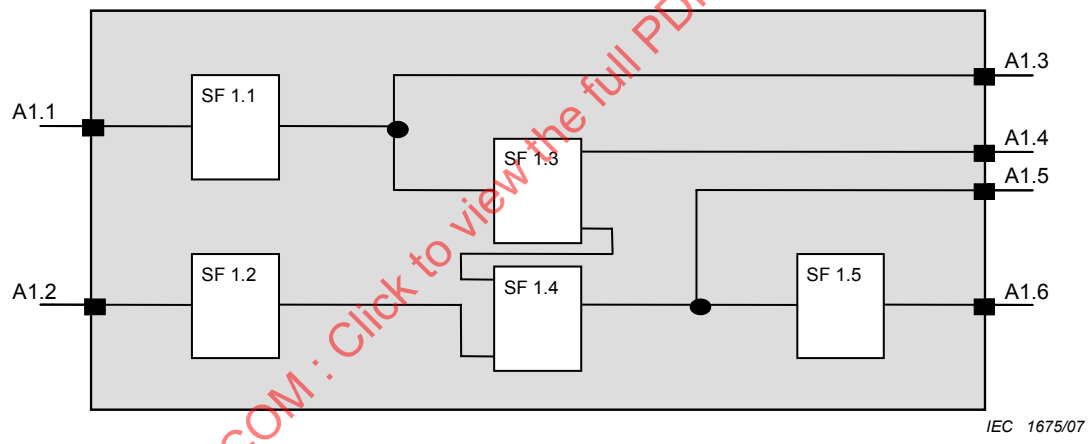


Figure B.3 – Functional model showing the functional terminals between the sub-functions

Rule: The functional context of the sub-function is shown in the functional model.

The functional model is the assignment of the sub-functions and terminals.

B.2.3 Determination of the parameters relating to the functions

B.2.3.1 Data for the document "system specification"

The data for the document "system specification" are used to determine the parameters for all sub-functions (SF). The parameters enable a quantitative description of the sub-functions (measurable at the sub-function terminals) and provide proof that these have been realized.

The terminals can then be determined at which the parameters are to take effect (SF terminals).

Subsequently, the terminals are determined at which the sub-function parameters are to take effect at the boundaries of the level under study.

The parameters that have been assigned to the sub-functions are documented in the test specification.

Rule: Each sub-function should be determined by at least one, or even several, parameters.

Table B.2 – Data for the document "test specification" (assignment of function to parameter)

Designation: Sample Item number: 12345678 Version: 01 Design level: K3 system					
Function	**Sub-function**	**Stimulus parameter**	**Stimulus terminal**	**Measurement parameter**	**Measurement terminal**
Function 1	SF1.1	Stim 1.1	A 1.1	Meas 1.1	A 1.3
		Stim 1.2	A 1.1	Meas 1.2	A 1.3
		Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2			Meas 2.1	
	SF1.3	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	Stim 1.5	A 1.2	Meas 4.1	A 1.5
		Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	Stim 1.6	A 1.2	Meas 5.1	A 1.6
Stimulus / measurement parameters shown in Figure B.5.					

B.3 Engineering design

B.3.1 Functional model, system specification

Once the functional structuring of the product has been completed, the hardware in which the functions are to be realized can be examined in the following steps:

– determine the product breakdown structure, taking the logistic and organizational requirements in the system specification into account;

– determine the product's function/sub-function breakdown, structured into design elements (hardware units);

– select those hardware units that should be replaceable by simple means (stipulation relating to logistic determination);

– confirm the functional model by inserting the determined hardware units;

– derive the respective terminals from the intersections of the functional links of the sub-functions with the boundaries of the hardware units.

The designations of the hardware unit terminals are given in the functional model (e.g. A1.5: terminal 5 in Figure B.4).

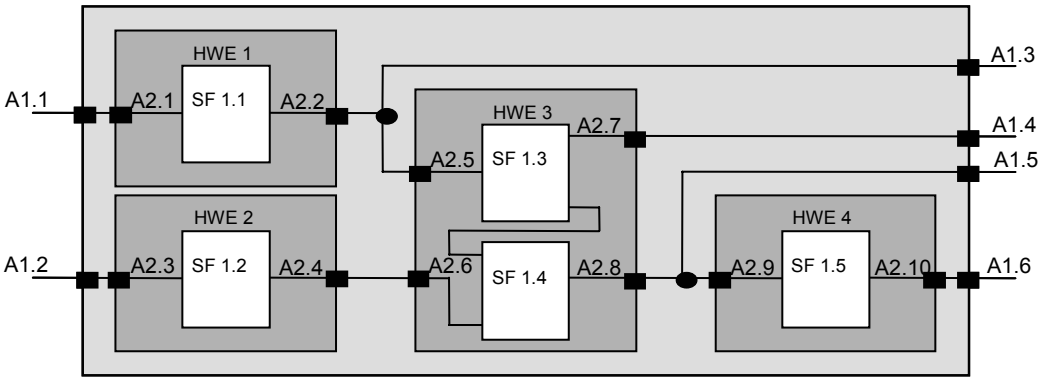


Figure B.4 – Functional model with inserted hardware units

The identified hardware units are to be assigned to a logistic level (LRU, SRU) in line with the logistic requirements of the system specification.

Table B.3 – Database with hardware units and logistic assignment added

Designation: Sample **Item number: 12345678** **Version: 01** **Design level: K3 system**							
Function	**Sub-function**	**HW unit**	**Log. assign.**	**Stimulus parameter**	**Stimulus terminal**	**Measurement parameter**	**Measurement terminal**
Function 1	SF1.1	1	LRU	Stim 1.1	A 1.1	Meas 1.1	A 1.3
				Stim 1.2	A 1.1	Meas 1.2	A 1.3
				Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2	2	LRU			Meas 2.1	
	SF1.3	3	LRU	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	3	LRU	Stim 1.5	A 1.2	Meas 4.1	A 1.5
				Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	4	LRU	Stim 1.6	A 1.2	Meas 5.1	A 1.6

B.4 Development of testability

B.4.1 Determination of test steps

In order to develop the required testability, the parameters of the sub-functions require verification.

A test step should be carried out to produce verification of a parameter.

In relation to one or several inputs (simultaneously), test steps are assigned to each parameter at the output.

In a test step, specific stimuli parameters are applied to an input of the function and measurements are made at the output where verification of the parameter is required.

The test steps are to be numbered clearly.

Rule: A test step should be assigned to each parameter having a terminal to the boundaries of the level under investigation.

Table B.4 – Database expanded to include the test steps

Designation: Sample	Item number: 12345678	Version: 01						
Design level: K3 system								
Function	**Sub-function**	**HW unit**	**Log. assign.**	**Test step**	**Stimulus parameter**	**Stimulus terminal**	**Measurement parameter**	**Measurement terminal**
Function 1	SF1.1	1	LRU	PS1	Stim 1.1	A 1.1	Meas 1.1	A 1.3
				PS2	Stim 1.2	A 1.1	Meas 1.2	A 1.3
				PS3	Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2	2	LRU				Meas 2.1[a]	
	SF1.3	3	LRU	PS4	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	3	LRU	PS5	Stim 1.5	A 1.2	Meas 4.1	A 1.5
				PS6	Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	4	LRU	PS7	Stim 1.6	A 1.2	Meas 5.1	A 1.6

[a] Parameters that are not accessible at the boundaries of the unit under investigation cannot be directly assigned to a test step. Such parameters can only be measured indirectly through other test steps across the overall function. In the example shown, parameter Meas 2.1 is measured indirectly via test steps 5 to 7.

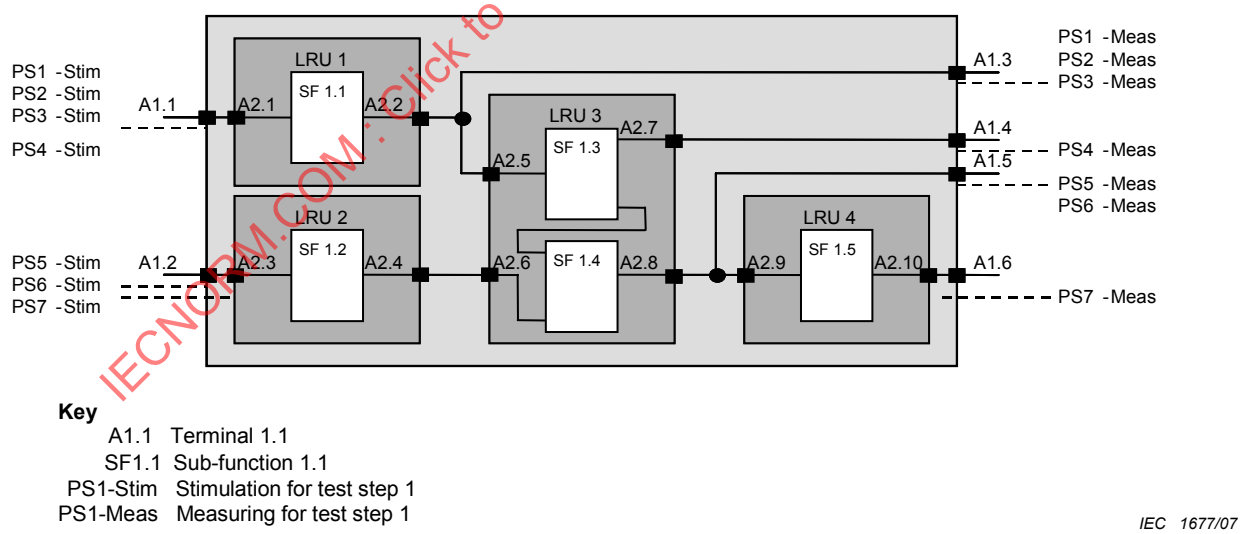


Figure B.5 – Functional model showing stimulation and measuring points

B.4.2 Determination of test paths

All sub-functions lying between the stimulation and measuring points of a test step and having an influence on the measurement are assigned to a test path.

Rule: A test path should be assigned to each test step.

If several parameters are to be verified at one terminal, where the same stimuli terminals are involved, the necessary test steps can be combined in a single test path (see Table B.5: test steps 1 to 3 are contained in test path 1).

The test paths should be numbered unambiguously.

Table B.5 – Database expanded to include the test paths

Designation: Sample	Item number: 12345678	Version: 01
Design level: K3 system		

Function	Sub-function	HW unit	Log. as-sign.	Test path	Test step	Stimulus parameter	Stimulus terminal	Measurement parameter	Measurement terminal
Function 1	SF1.1	1	LRU	PP1	PS1	Stim 1.1	A 1.1	Meas 1.1	A 1.3
				PP1	PS2	Stim 1.2	A 1.1	Meas 1.2	A 1.3
				PP1	PS3	Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2	2	LRU					Meas 2.1	
	SF1.3	3	LRU	PP2	PS4	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	3	LRU	PP3	PS5	Stim 1.5	A 1.2	Meas 4.1	A 1.5
				PP3	PS6	Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	4	LRU	PP4	PS7	Stim 1.6	A 1.2	Meas 5.1	A 1.6

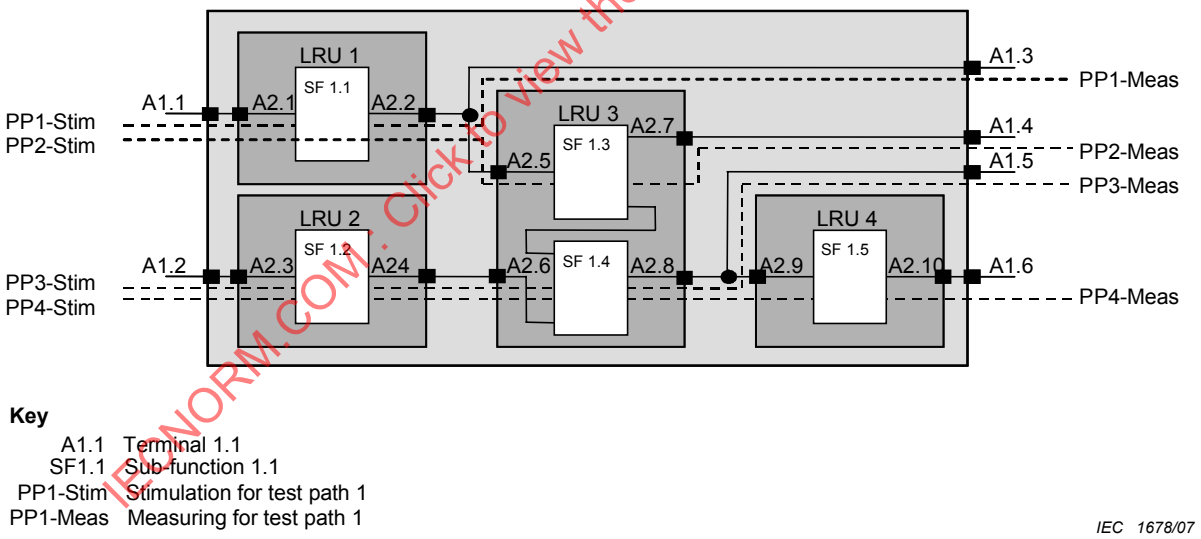
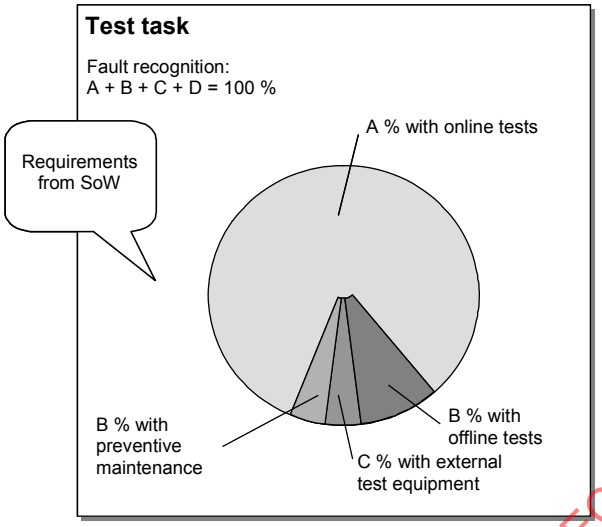


Figure B.6 – Functional model showing test paths

In Figure B.6, the functional model and database have been expanded to include the test paths.

B.4.3 Assignment to the respective portion of the test task

Fault recognition is carried out by means of the tests shown in Figure B.7.



Key
Portion A (%) Tests during operation (online tests)
Portion B (%) Tests under test conditions, without external test equipment (offline test)
Portion C (%) Test under test conditions, with external test equipment
Portion D (%) Preventive maintenance (preventive replacement of hardware units)

IEC 1679/07

Figure B.7 – Portions of the test task

The individual test paths are to be assigned to a respective portion (A, B, C or D) on the basis of the functional model and are to be entered in the database (see Table B.6).

Table B.6 – Database expanded to include the test task portions

Designation: Sample		Item number: 12345678		Version: 01						
Design level: K3 system										
Function	**Sub-function**	**HW unit**	**Log. assign.**	**Test path**	**Test step**	**Section of test task**	**Stimulus parameter**	**Stimulus terminal**	**Measurement parameter**	**Measurement terminal**
Function 1	SF1.1	1	LRU	PP1	PS1	Section B	Stim 1.1	A 1.1	Meas 1.1	A 1.3
				PP1	PS2	Section B	Stim 1.2	A 1.1	Meas 1.2	A 1.3
				PP1	PS3	Section B	Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2	2	LRU						Meas 2.1	
	SF1.3	3	LRU	PP2	PS4	Section A	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	3	LRU	PP3	PS5	Section C	Stim 1.5	A 1.2	Meas 4.1	A 1.5
				PP3	PS6	Section C	Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	4	LRU	PP4	PS7	Section A	Stim 1.6	A 1.2	Meas 5.1	A 1.6

In Table B.6, data for the test specification has been expanded to include the test task sections.

B.5 Assessment of fault recognition

B.5.1 Methodology for the calculation of fault recognition

The database is to be expanded by adding further columns.

These columns will contain the designations of the terminals for all hardware units.

It is to be determined how many terminals and hardware units there are and this number is to be entered in the respective totals column (see Table B.7: 10 terminals and 4 HW units).

Table B.7 – Determination of how many terminals and hardware units there are

HW unit / Terminal	LRU1		LRU2		LRU3				LRU4		Σ Terminals	Σ HW unit
	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4

For each test path, those terminals that are covered by this test path are to be marked with an "X".

Test steps mentioned more than once should be taken into account only once within a test path.

Table B.8 – Matrix showing coverage of terminals and paths

HW unit / Terminal			**LRU1**		**LRU2**		**LRU3**				**LRU4**		**Σ Terminals**	**Σ HW unit**
			2.1	**2.2**	**2.3**	**2.4**	**2.5**	**2.6**	**2.7**	**2.8**	**2.9**	**2.10**	**10**	**4**
…	Test step	Test path												
…	PS1	PP1	X	X	—	—	—	—	—	—	—	—		
…	PS2													
…	PS3													
…														
…	PS4	PP2	X	X	—	—	X	—	X	—	—	—		
…	PS5													
…	PS6	PP3	—	—	X	X	—	X	—	X	—	—		
…	PS7	PP4	—	—	X	X	—	X	—	X	X	X		

B.5.2 Characteristic value for the quality of the fault recognition (FR) during operation

From the database, all those test paths are to be determined for which the entry "portion A" has been made in the "tests during operation" section of the test task (see Table B.6). These are the test paths that can make a contribution to the on-line test.

Using this reduced quantity of data, the characteristic value for the quality of the fault recognition during operation is to be determined.

A check is to be made as to whether each terminal is covered by at least one test path. If at least one "X" is to be found in the column for a particular terminal, then a "1" is to be entered for this terminal in the line "Fault recognizable via portion A?".

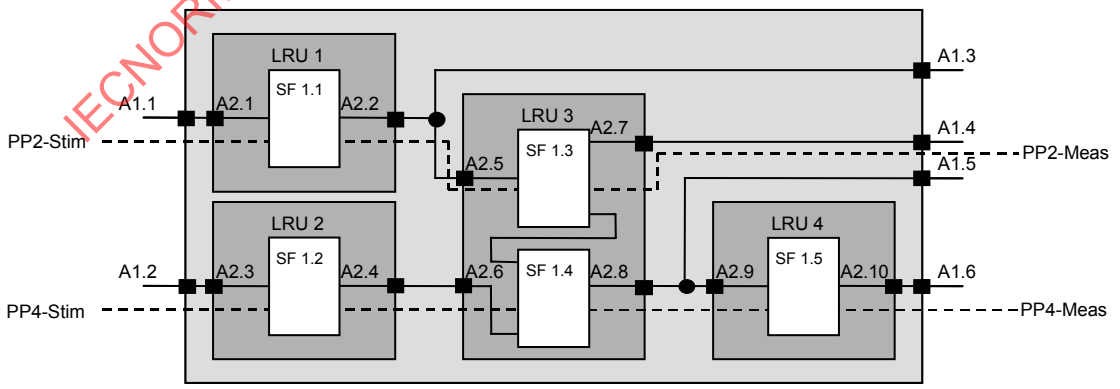
EXAMPLE: Terminal A 2.5 is covered by test path 2 (PP2) (see Table B.9). As terminal A 2.5 is covered by test path 2, a fault occurring at this terminal can be recognized.

The sum of the terminals at which a fault is recognizable is entered in the sum field.

Table B.9 – Determination of the characteristic value for the quality of the fault recognition (FR) during operation (section A)

HW unit Terminal			LRU1		LRU2		LRU3				LRU4		Σ Terminals	Σ HW unit	Charactеristic value
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$
…	Test step	Test path													
…	PS1	PP1	-	-	-	-	-	-	-	-	-				
…	PS2														
…	PS3														
…															
…	PS4	PP2	X	X	-	-	X	-	X	-	-	-			
…	PS5														
…	PS6	PP3	-	-	-	-	-	-	-	-	-	-			
…	PS7	PP4	-	-	X	X	-	X	-	X	X	X			
Fault recognizable via portion A?			1	1	1	1	1	1	1	1	1	1	10		100 %

From the functional model, in which all test paths have been entered, all those test paths are to be extracted which are to be allocated to the "tests during operation" portion of the test task ("section A") (see Figure B.8).



Key

A1.1 Terminal 1.1
SF1.1 Sub-function 1.1
PP2-Stim Stimulation for test path 2
PP2-Meas Measuring for test path 2

IEC 1680/07

Figure B.8 – Functional model showing the test paths of portion A

The characteristic value for the quality of the fault recognition during operation $FR_{(A)}$ is determined from the ratio of the sub-functions and/or terminals covered by the selected test paths to the actual terminals (see formula below).

$$FR_{(A)} = \frac{\text{Number of terminals for sub-functions covered by portion A test paths}}{\text{Number of actual terminals for sub-functions}} \times 100\ [\%]$$

The characteristic value established should be recorded in the database.

EXAMPLE: The terminals A2.1 to 2.10 for the sub-functions SF1.1 to SF1.5 are covered by the section A test paths (PP2 and PP4).

$$FR_{(A)} = \frac{\text{10 terminals for sub-functions by test paths}}{\text{10 actual terminals for sub-functions}} \times 100 = 100\ [\%]$$

B.5.3 Characteristic value for the quality of the fault recognition (*FR*) under test conditions

All sections of the test tasks (Portions A + B + C + D) may be used for fault recognition under test conditions.

Using this quantity of data, the characteristic value for fault recognition under test conditions is to be determined.

A check is made as to whether each terminal is covered by at least one test path. If at least one "X" is to be found in the column for a particular terminal, then a "1" is to be entered for this terminal in the line "Fault recognizable via portion A + B + C + D?"

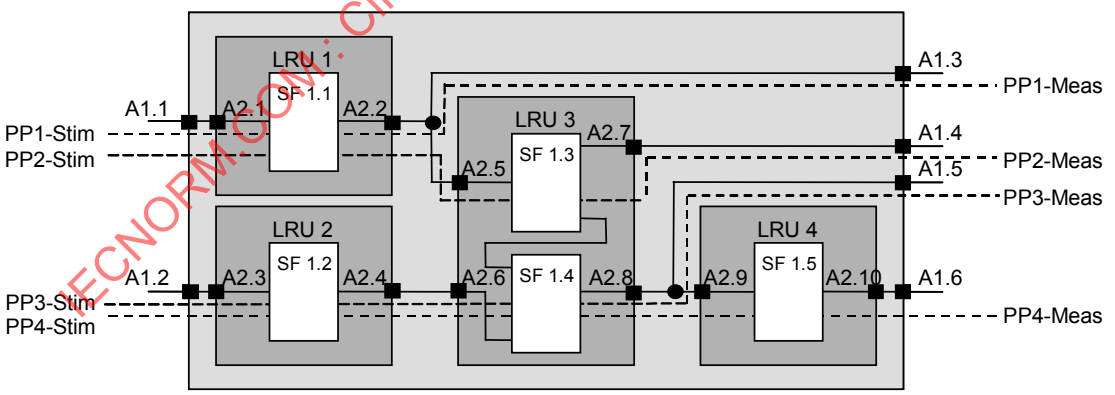
EXAMPLE: Terminal 2.5 is covered by test path 2 (PP2) (see Table B.10). As terminal 2.5 is covered by test path 2, a fault occurring at this terminal can be recognized.

The sum of the terminals at which a fault is recognizable is entered in the sum field.

Table B.10 – Determination of the characteristic value for the quality of the fault recognition (*FR*) under test conditions (Portions A+B+C+D)

HW unit			LRU1		LRU2		LRU3				LRU4		Σ	Σ	Characteristic values	
Terminal			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	Terminals 10	HW unit 4	$FR_{(A)}$	$FR_{(A+B+C+D)}$
...	Test step	Test path														
...	PS1	PP1	X	X	—	—	—	—	—	—	—	—				
...	PS2															
...	PS3															
...																
...	PS4	PP2	X	X	—	—	X	—	X	—	—	—				
...	PS5															
...	PS6	PP3	—	—	X	X	—	X	—	X	—	—				
...	PS7	PP4	—	—	X	X	—	X	—	X	X	X				
Fault recognizable by means of section A?			1	1	1	1	1	1	1	1	1	1	10		100 %	
Fault recognizable by means of section A + B + C + D?			1	1	1	1	1	1	1	1	1	1	10			100 %

All test paths should be entered in the functional model.



Key

A1.1 Terminal 1.1
SF1.1 Sub-function 1.1
PP1-Stim Stimulation for test path 1
PP1-Meas Measuring for test path 1

IEC 1681/07

Figure B.9 – Functional model showing the test paths of portions A + B + C + D

The characteristic value for the quality of the fault recognition under test conditions $FR_{(A+B+C+D)}$ is determined from the ratio of the terminals covered by the test paths to the actual terminals (see formula below).

$$FR_{(A+B+C+D)} = \frac{\text{Number of terminals for sub-functions covered by test paths in Portions A + B + C + D}}{\text{Number of actual terminals for sub-functions}} \times 100\ [\%]$$

The characteristic value established should be recorded in the database.

EXAMPLE: The terminals A2.1 to 2.10 for the sub-functions SF1.1 to SF1.5 are covered by the test paths in portions A + B + C + D (PP1 to PP4).

$$FR_{(A+B+C+D)} = \frac{\text{10 terminals for sub-functions by test paths}}{\text{10 actual terminals for sub-functions}} \times 100 = 100\ [\%]$$

B.6 Assessment of fault localization

B.6.1 Methodology for the calculation of fault localization

Assessment of fault localization is carried out on the basis of the coverage matrix.

Table B.11 – Coverage matrix

HW unit / Terminal			LRU1		LRU2		LRU3				LRU4		Σ Terminals	Σ HW unit	Characteristic value		
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	
…	Test step	Test path															
…	PS1	PP1	X	X	—	—	—	—	—	—	—	—					2^0
…	PS2																
…	PS3																
…																	
…	PS4	PP2	X	X	—	—	X	—	X	—	—	—					2^1
…	PS5																
…	PS6	PP3	—	—	X	X	—	X	—	X	—	—					2^2
…	PS7	PP4	—	—	X	X	—	X	—	X	X	X					2^3
			3	3	12	12	2	12	2	12	8	8					

Weighting in binary coding 2^0 to 2^n is assigned to each test path in a row.

The columns for the terminals are interpreted as binary numbers (“X” corresponds to "1"; “—“ corresponds to "0") and are entered in the coding line in decimal form.

Thus for each terminal from Table B.11 a coding as shown in Table B.12 is calculated.

Table B.12 – Coding of terminals

HW unit	LRU1		LRU2		LRU3				LRU4	
Terminal	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10
Coding	3	3	12	12	2	12	2	12	8	8

The coding of the column for the terminal of a hardware unit is to be checked against all other codings of the remaining hardware units.

If the coding in question occurs only once, then for this terminal a "1" is to be entered in the line "Unambiguously locatable?".

EXAMPLE: Compare the coding (2) assigned to terminal A 2.5 with those of the other terminals for hardware unit 1 (3 and 3), for hardware unit 2 (12 and 12) and for hardware unit 4 (8 and 8). As the coding for terminal A 2.5 occurs only once, this terminal can be unambiguously localized in the event of a fault.

The sum of the unambiguously locatable terminals is entered in the sum field.

Table B.13 – Sum field

Coding	3	3	12	12	2	12	2	12	8	8				
Unambiguously locatable?	1	1	—	—	1	—	1	—	1	1	6			
Unambiguously locatable hardware unit $FL_{(L1)}$		1								1		2		

Once all the terminals of a hardware unit have been determined as locatable, then a "1" is to be entered in the line "Unambiguously locatable hardware unit" of the respective hardware unit.

EXAMPLES: The method of determining fault localization can be explained more clearly by means of the following examples in Figure B.10 and B.11.

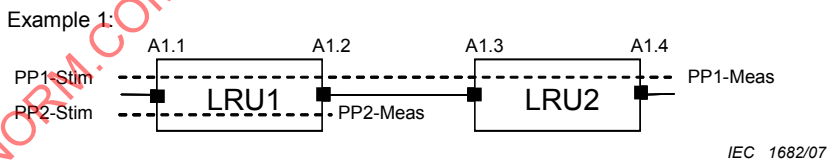


Figure B.10 – Functional model of case study 1

The following matrix is to be derived from the functional model given in Table B.14.

Table B.14 – Fault localization matrix of case study 1

	LRU1		LRU2		Σ Terminals	Σ HW unit	Characteristic value	
	A1.1	A1.2	A1.3	A1.4	4	2	*FL*	
PP1	X	X	X	X				2^0
PP2	X	X	—	—				2^1
Coding	3	3	1	1				
Unambiguously locatable	1	1	1	1	4		100 %	
Unambiguously locatable hardware unit		1		1		2	100 %	
Locatable in conjunction with two hardware units						0	0 %	
Locatable in conjunction with n hardware units						0	0 %	

An unambiguous fault localization for the terminals is ensured through the test paths selected.

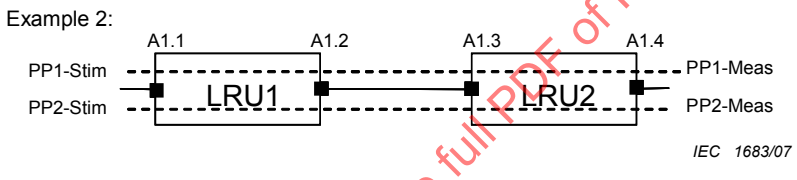


Figure B.11 – Functional model of case study 2

The following matrix is to be derived from the functional model:

Table B.15 – Fault localization matrix of case study 2

	LRU1		LRU2		Σ Terminals	Σ HW unit	Characteristic value	
	A1.1	A1.2	A1.3	A1.4	4	2	*FL*	
PP1	X	X	X	X				2^0
PP2	X	X	X	X				2^1
Coding	3	3	3	3				
Unambiguously locatable	—	—	—	—	0		0 %	
Unambiguously locatable hardware unit		—		—		0	0 %	
Locatable in conjunction with two hardware units		1		1		2	100 %	
Locatable in conjunction with n hardware units						0	0 %	

An unambiguous fault localization for the terminals is not ensured through the test paths selected.

B.6.2 Characteristic value for the quality of the fault localization (*FL*)

The principle demonstrated up to now is also to be applied when determining the characteristic value for the quality of the fault localization (*FL*) (see Table B.16).

Table B.16 – Determining the characteristic value for the quality of fault localization (*FL*)

HW unit / Terminal			LRU1		LRU2		LRU3				LRU4		Σ Terminals	Σ HW unit	Characteristic values			
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	*FL*	
…	Test step	Test path																
…	PS1	PP1	X	X	—	—	—	—	—	—	—	—						2^0
…	PS2																	
…	PS3																	
…																		
…	PS4	PP2	X	X	—	—	X	—	X	—	—	—						2^1
…	PS5																	
…	PS6	PP3	—	—	X	X	—	X	—	X	—	—						2^2
…	PS7	PP4	—	—	X	X	—	X	—	X	X	X						2^3
Coding			3	3	12	12	2	12	2	12	8	8						
Unambiguously locatable?			1	1	—	—	1	—	1	—	1	1	6				60%	

The characteristic value for the quality of the fault localization (*FL*) is determined from the ratio of all the terminals that can be used for fault localization ("1" in locatable line) to all existing terminals.

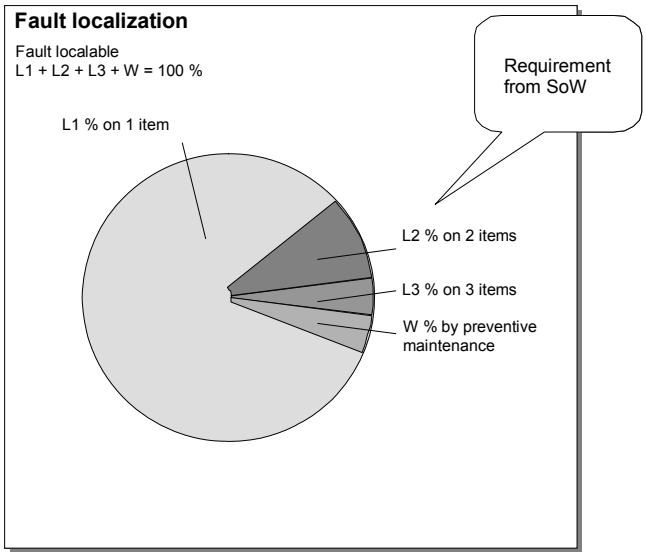
$$FL = \frac{\text{Number of terminals usable for fault localization}}{\text{of all existing terminals for sub-functions}} \times 100\ [\%]$$

In the example, *FL* = 60 %

B.6.3 Relation to fault location (hardware unit) and unambiguity

An assessment is made in relation to each hardware unit as to whether a "yes" has been entered in the "Locatable" line for all its terminals.

Reference should be made to the system specification to establish what degree of ambiguity should not be exceeded in the fault localization on hardware units.



Key
Portion L1 (%) Localization of 1 item
Portion L2 (%) Localization of 2 items
Portion L3 (%) Localization of 3 items
Portion W (%) Preventive maintenance (preventive replacement of hardware units)

IEC 1684/07

Figure B.12 – Fault localization portions

Table B.17 is to be supplemented by the appropriate number of lines (in each case "Locatable on *n* hardware units").

In the example, the SoW states that a maximum of three hardware units may be involved in one fault.

In the line "Locatable on one hardware unit" a "1" is to be entered if all terminals of the hardware unit have been given the assessment "yes" in the "Locatable" line.

In each column for which a "no" has been entered in the "Locatable" line a reference is to be made to the hardware units involved in the fault.

Table B.17 – Determination of the locatability of the hardware units

HW unit / Terminal			LRU1		LRU2		LRU3				LRU4		Σ Terminals	Σ HW unit	Characteristic value			
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	FL	
…	Test step	Test path																
…	PS1	PP1	X	X	—	—	—	—	—	—	—	—						2^0
…	PS2																	
…	PS3																	
…	PS4	PP2	X	X	—	—	X	—	X	—	—	—						2^1
…	PS5																	
…	PS6	PP3	—	—	X	X	—	X	—	X	—	—						2^2
…	PS7	PP4	—	—	X	X	—	X	—	X	X	X						2^3
Coding			3	3	12	12	2	12	2	12	8	8						
Unambiguously locatable?			1	1	—	—	1	—	1	—	1	1	6				60 %	
Unambiguously locatable hardware unit $FL_{(L1)}$				1								1		2			50 %	
Locatable in conjunction with two hardware units $FL_{(L2)}$						1			1					2			50 %	
Locatable in conjunction with three hardware units $FL_{(L3)}$														—			0 %	

The percentage distribution of the locatability over one, two or three hardware units in ratio to the total number of hardware units at the level under investigation is calculated in the following manner:

$$FL_{\mathrm{HWE(Ln)}} = \frac{\text{Number of hardware units locatable on } n}{\text{Total number of hardware units}} \times 100\ [\%]$$

In the example,

- $FL_{\mathrm{HWE\ (L1)}}$ = 50 %
- $FL_{\mathrm{HWE\ (L2)}}$ = 50 %
- $FL_{\mathrm{HWE\ (L3)}}$ = 0 %
- $FL_{\mathrm{HWE\ (W)}}$ = 0 %

B.6.4 Ways of improving the characteristic value for the quality of fault localization (*FL*)

The fault localization may be improved by taking various steps:

– design changes by introducing additional sub-functions and/or terminals for test purposes (see Figure B.13, terminal A1.7);

– additional test paths by defining appropriate test and simulation data (see Table B.18, test path PP5).

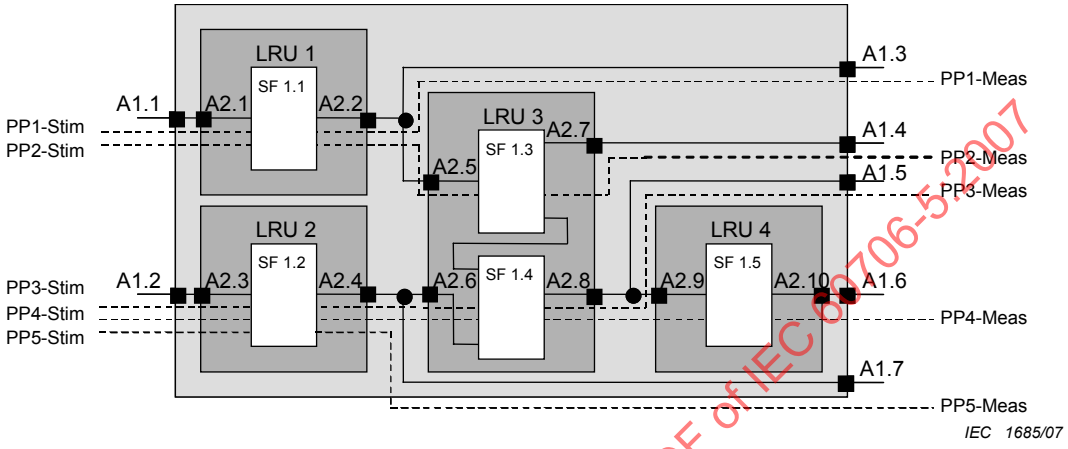


Figure B.13 – Functional model with additional stimulation and measuring points

Table B.18 – Data table expanded to include test path PP 5

Designation: Sample Item number: 12345678 Version: 02 Design level: K3 system										
Function	**Sub-function**	**HW unit**	**Log. as-sign.**	**Test path**	**Test step**	**Portion of test task**	**Stimulus parameter**	**Stimulus terminal**	**Measurement parameter**	**Measurement terminal**
Function 1	SF1.1	1	LRU	PP1	PS1	Section B	Stim 1.1	A 1.1	Meas 1.1	A 1.3
				PP1	PS2	Section B	Stim 1.2	A 1.1	Meas 1.2	A 1.3
				PP1	PS3	Section B	Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2	2	LRU	PP5	PS8	Section C	Stim 1.7	A 1.2	Meas 2.1	A 1.7
	SF1.3	3	LRU	PP2	PS4	Section A	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	3	LRU	PP3	PS5	Section C	Stim 1.5	A 1.2	Meas 4.1	A 1.5
				PP3	PS6	Section C	Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	4	LRU	PP4	PS7	Section A	Stim 1.6	A 1.2	Meas 5.1	A 1.6

Table B.19 – Determination of the locatability of the hardware units, including additional test path 5

HW unit			LRU1		LRU2		LRU3				LRU4		Σ Terminals	Σ HW unit	Characteristic value			
Terminal			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	FL	
…	Test step	Test path																
…	PS1	PP1	X	X	—	—	—	—	—	—	—	—						2^0
…	PS2																	
…	PS3																	
…	PS8	PP5	—	—	X	X	—	—	—	—	—	—						2^1
…	PS4	PP2	X	X	—	—	X	—	X	—	—	—						2^2
…	PS5																	
…	PS6	PP3	—	—	X	X	—	X	—	X	—	—						2^3
…	PS7	PP4	—	—	X	X	—	X	—	X	X	X						2^4
Coding			5	5	26	26	4	24	4	24	16	16						
Unambiguously locatable?			1	1	1	1	1	1	1	1	1	1	10				100 %	
Unambiguously locatable hardware unit $FL_{(L1)}$				1		1			1			1		4			100 %	
Locatable in conjunction with 2 hardware units $FL_{(L2)}$														—			0 %	
Locatable in conjunction with 3 hardware units $FL_{(L3)}$														—			0 %	

The percentage distribution of the locatability over one, two or three hardware units in ratio to the total number of hardware units at the level under investigation is calculated using the following equation:

$$FL_{\mathrm{HWE(Ln)}} = \frac{\text{Number of hardware units locatable on } n}{\text{Total number of hardware units}} \times 100\ [\%]$$

In the example:

- $FL_{\mathrm{HWE\ (L1)}}$ = 100 %
- $FL_{\mathrm{HWE\ (L2)}}$ = 0 %
- $FL_{\mathrm{HWE\ (L3)}}$ = 0 %
- $FL_{\mathrm{HWE\ (W)}}$ = 0 %

B.7 Verification of testability

B.7.1 Implementation of the verifications

The contractor should provide proof that the prescribed fault recognition and localization are achieved.

Proof can be provided within the scope of development acceptance tests since testability is a requirement placed on the system.

Verification may be provided in two different ways.

- Verification by analysis

Verification by analysis takes place within the scope of the design review and takes the form of a testability record relating to the product's current test specification. This verification can therefore be repeated at any point in the product's life cycle, e.g. during production or after specification changes have been incorporated, etc.

- Verification by tests

If this verification by tests on the product hardware is required in the SoW, then it will be carried out during acceptance of the development result and the test specification provides the basis of the verification.

If the prescribed values cannot be verified, then the customer is to be consulted in order to achieve a corrective action, or a contract modification should be agreed on.

B.7.2 Methodology for verification

To produce verification by means of demonstration, test paths are selected according to the following criteria:

- Mission-critical – including safety-relevant – test paths

These paths are defined in line with the requirements in the system specification. Of all existing test paths, verification is to be provided for all those that are classified as mission-critical (e.g. in accordance with the FMECA). It is an essential requirement that fault recognition can be carried out for these test paths.

- Failure-dependent test paths (Lambda)

In the SoW where the customer requires a variety of failure-dependent test paths for verification, then the expected failure rates of the LRU/SRU are needed. Breakdown of the product failure rate into the respective shares for the LRUs to be defined by the developer may also be stipulated in the form of specifications by the customer and/or the developer himself may state these, depending on the failure rate assessment.

- Stochastic selection of paths

From the test paths that have not yet been verified, a certain number of statistically determined paths are selected and verified.

The test paths selected are noted in the verification record.

Proof of testability is provided on the basis of a verification record containing test paths that have been selected according to the above-mentioned criteria.

The verifications are provided by simulating a fault on one of the hardware units covered by the respective test path.

Table B.20 – Verification record

Designation: Sample **Item number: 12345678** **Version: 01** **Design level: K3 system**									
Function	**Sub-function**	**HW unit**	**Test path**	**Test step**	**1/MTBF λ**	**Critical**	**Simulate?**	**Criterion**	**Deviation from parameter recognized?**
Function 1	SF1.1	LRU1	PP1	PS1	1/1000		Yes	High Lambda	
				PS2					
				PS3					
	SF1.2	LRU2			1/9000				
	SF1.3	LRU3	PP2	PS4	1/2500		No		
	SF1.4	LRU3	PP3	PS5	1/2000		Yes	Stochastic	
				PS6					
	SF1.5	LRU4	PP4	PS7	1/1500	Yes	Yes	Critical fault	

As a result, a record is made of the parameter deviations. If a deviation from the parameters is identified, then the documented test paths correspond to those realized in the system.

The verification record confirms that the documented testability corresponds to that realized in the system. Deviations are not allowed.

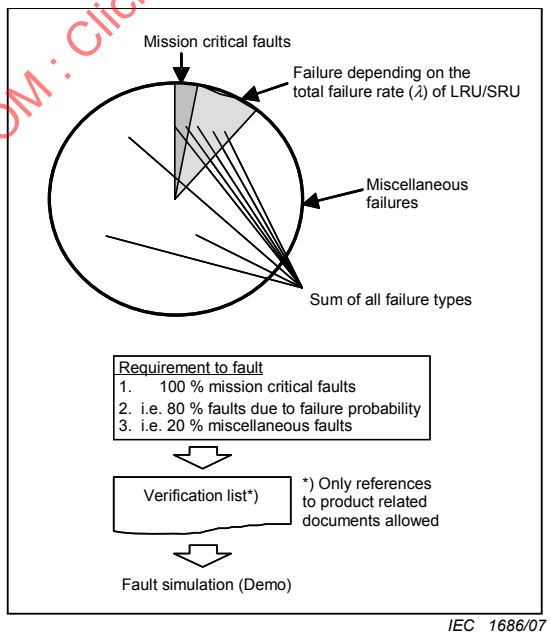


Figure B.14 – Selection criteria for verification

B.8 Documents

B.8.1 General

The central "document" for describing testability is the functional model.

All information that is stored in the functional model is based on the documents system specification, test specification and extended block diagram and is updated throughout the product's life cycle.

These documents and the functional model should be stored in a data module, which amongst other things means that all information packages have to be stored in a common source database (CSDB) and be addressable by means of a data module code.

B.8.2 **System specification** (see example in Table 21)

The document "system specification" contains a written description of the functionality to be realized.

Table B.21 – Example of the document "system specification"

Designation: Sample **Item number: 12345678** **Version: 01** **Design level: K3 system**	
Function	**Sub-function**
Function 1	SF1.1 SF1.2 SF1.3 SF1.4 SF1.5
Function 2	Not investigated in example
Function 3	Not investigated in example

B.8.3 Test specification

The document "Test specification" contains the parameters needed in order to realize the required functionality.

Table B.22 – Example of the document "test specification"

Designation: Sample Item number: 12345678 Version: 01 Design level: K3 system										
Function	**Sub-function**	**HW unit**	**Log. assign.**	**Test path**	**Test step**	**Portion of test task**	**Stimulus parameter**	**Stimulus terminal**	**Measurement parameter**	**Measurement terminal**
Function 1	SF1.1	1	LRU	PP1	PS1	Section B	Stim 1.1	A 1.1	Meas 1.1	A 1.3
				PP1	PS2	Section B	Stim 1.2	A 1.1	Meas 1.2	A 1.3
				PP1	PS3	Section B	Stim 1.3	A 1.1	Meas 1.3	A 1.3
	SF1.2	2	LRU						Meas 2.1	
	SF1.3	3	LRU	PP2	PS4	Section A	Stim 1.4	A 1.1	Meas 3.1	A 1.4
	SF1.4	3	LRU	PP3	PS5	Section C	Stim 1.5	A 1.2	Meas 4.1	A 1.5
				PP3	PS6	Section C	Stim 1.5	A 1.2	Meas 4.2	A 1.5
	SF1.5	4	LRU	PP4	PS7	Section A	Stim 1.6	A 1.2	Meas 5.1	A 1.6

B.8.4 Extended block diagram (see Figure B.15)

This is a block diagram expanded to include the test paths. The test paths should be marked in an unambiguous manner. In case of need, several identical block diagrams may be used in order to demonstrate the individual test paths.

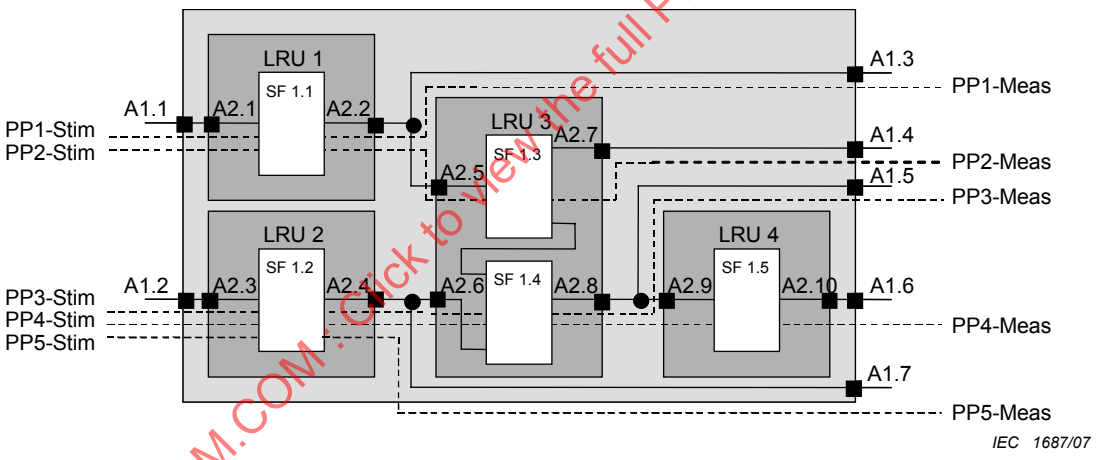


Figure B.15 – Functional model shown in the form of an extended block diagram

The completed block diagram provides all basic information for diagnostic testing. Depending on the size of the system to be tested diagnostic testing may be conducted with computer based software tools using the data tables such as Table B.22, while manual diagnostic testing will primarily use the detailed extended block diagram.

B.8.5 Verification record

Proof of testability is provided on the basis of a verification record containing the test paths that are to be verified.

The verification record contains information as shown in Table B.23.

Table B.23 – Verification record

Designation: Sample	**Item number: 12345678**			**Version: 01**					
Design level: K3 system									
Function	**Sub-function**	**HW unit**	**Test path**	**Test step**	**1/MTBF λ**	**Critical ?**	**Simulate?**	**Criterion**	**Deviation from parameter recognized?**
Function 1	SF1.1	LRU1	PP1	PS1	1/1000		Yes	High Lambda	
				PS2					
				PS3					
	SF1.2	LRU2			1/9000				
	SF1.3	LRU3	PP2	PS4	1/2500		No		
	SF1.4	LRU3	PP3	PS5	1/2000		Yes	Stochastic	
				PS6					
	SF1.5	LRU4	PP4	PS7	1/1500	Yes	Yes	Critical fault	

This verification is to be carried out on the product hardware. If this verification is required in the SoW, then it is to be performed during acceptance (see M3 in Figure 3) of the development result. Once again, the test specification is to provide the basis for this verification. Simulation is accomplished by means of non-destructive interventions in the hardware units and/or, where necessary, via software.

Bibliography

IEC 60300-1:2003, *Dependability management – Part 1: Dependability management systems*

IEC 60300-2:2004, *Dependability management – Part 2: Guidelines for dependability management*

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

IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

MAINTENABILITÉ DE MATÉRIEL –

Partie 5: Testabilité et tests pour diagnostic

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60706-5 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette seconde édition annule et remplace la première édition publiée en 1994, et constitue une révision technique. Elle élargit le champ de la première édition, et fournit plus de détails sur les techniques et les systèmes présentés de façon générale dans la première édition.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
56/1211/FDIS	56/1231/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

Une liste de toutes les parties de la CEI 60706, présentée sous le titre général *Maintenabilité de matériel*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

La testabilité est un élément important pour l'exploitation et la maintenance d'un système ou d'un équipement, et a un effet significatif sur sa disponibilité et sa maintenabilité. Des tests pour diagnostic peuvent être effectués manuellement ou bien à l'aide d'équipements de test qui peuvent être dotés de divers niveaux d'automatisation. La conception optimale pour la testabilité nécessite une étroite coopération entre les organisations de conception, d'exploitation et de maintenance. Cette norme a pour but de mettre en lumière les divers aspects de la testabilité et des tests de diagnostic et d'assurer leur coordination dans le temps.

Dans cette norme, les dispositifs à considérer au regard de leur conception pour la testabilité peuvent être des systèmes, des équipements ou unités fonctionnelles qui font l'objet d'un contrat, et qu'on désignera sous le terme de « produits». Chaque produit doit accomplir les fonctions requises qu'il convient de vérifier pendant les phases de développement et de production et de retenir sur toute la durée du cycle de vie. Afin de maintenir la fonctionnalité d'un produit, il convient de connaître le statut fonctionnel de chaque sous-fonction à tout moment lorsque le produit est en condition de fonctionnement. En cas de défaillance, il convient d'agir pour s'assurer que le défaut est reconnu et l'élément défectueux localisé. Cette exigence placée sur la testabilité d'un produit peut paraître assez simple, mais si elle n'est pas considérée au début du développement du produit, la réalisation suivante résultera dans l'augmentation significative du travail et des coûts. Si toutes les exigences sont connues au début du développement, l'ingénieur de développement peut spécifier la caractéristique fonctionnelle de « testabilité » sans trop d'effort supplémentaire et par conséquent réaliser des économies importantes, par exemple en minimisant le nombre d'étapes de test pour vérifier les résultats de développement. L'expérience a montré que les coûts et efforts supplémentaires dans la phase de développement peuvent être récupérés, par exemple dans la phase de production, si le matériel d'essai disponible peut être utilisé. Une détection de panne fiable et des coûts bas de maintenance en fonctionnement augmentent considérablement la valeur du marché d'un produit testable.

Les technologies appliquées aux produits couverts par cette norme étant d'un domaine très large, ce document a été écrit sans considérations relatives aux technologies et techniques. Par conséquent, cette norme fournit uniquement une base d'évaluation pour établir des calculs et l'approche de base pour atteindre la testabilité exigée d'un produit. La réalisation technique d'une détection de panne et d'une localisation de panne dans le produit est la tâche de l'ingénieur de développement du produit et doit être réalisée suivant les règles de l'art en vigueur au moment du développement du produit. Par conséquent, la réalisation du test nécessaire sous forme matérielle ou logicielle n'a pas grande importance, mais il est essentiel que toutes les fonctions soient vérifiées par le biais de chemins de test et que les valeurs de caractéristiques établies pour la testabilité correspondent à des valeurs d'objectif spécifié. S'il existe des écarts par rapport aux valeurs ciblées, il convient d'agir pour assurer que ces valeurs sont atteintes. Il convient que ces actions se produisent à un stade précoce du développement avant la fin de la conception.

MAINTENABILITÉ DE MATÉRIEL –

Partie 5: Testabilité et tests pour diagnostic

1 Domaine d'application

Le but de cette partie de la CEI 60706 est de

- fournir des indications pour la prise en considération, très tôt, des aspects de testabilité en conception et développement;
- aider dans la détermination de procédures de test efficaces en tant que partie intégrante de l'exploitation et de la maintenance.

Cette norme internationale peut être appliquée à tous types de produits y compris les produits sur étagère (COTS). A cet égard, que le produit relève d'une technologie mécanique, hydraulique, électrique ou d'une autre technologie n'a pas d'importance. De plus, cette norme internationale s'applique au développement de tout produit, avec pour but de concevoir les caractéristiques de produit pour qu'elles soient vérifiables (testables).

L'objectif de cette norme internationale est d'assurer que les pré-requis relatifs à la testabilité des produits sont définis dans les phases préliminaires du développement, exposés par le client, mis en œuvre, documentés et vérifiés pendant le développement.

Cette norme internationale fournit également des méthodes pour mettre en application et évaluer la testabilité comme partie intégrante de la conception de produit. Il est recommandé que la documentation sur la testabilité du produit soit mise à jour tout au long du cycle de vie du produit.

2 Références normatives

Les documents référencés suivants sont indispensables pour l'application de ce document. Pour des références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition du document référencé (y compris les amendements) qui s'applique.

CEI 60050-191, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60706-2, *Maintenabilité de matériel – Partie 2: Exigences et études de maintenabilité pendant la phase de conception et de développement*

CEI 60706-3, *Maintenabilité de matériel – Partie 3: Vérification et recueil, analyse et présentation des données*

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

3 Termes, définitions et acronymes

3.1 Termes et définitions

Pour les besoins de ce document, les termes et définitions de la CEI 60050-191 s'appliquent avec les suivants:

3.1.1
test intégré
TI
capacité intégrée à une entité soumise au test permettant une détection et une localisation de panne automatiques

3.1.2
équipement de test intégré
ETI
matériel et/ou logiciel assigné à l'équipement de test intégré

3.1.3
produit sur étagère
COTS
entités immédiatement disponibles dans le commerce

3.1.4
criticité
signification attachée à un dysfonctionnement

NOTE La criticité s'exprime en degré: plus le degré est élevé, plus les conséquences à attendre du dysfonctionnement sont graves.

3.1.5
profondeur du test
spécification du niveau auquel l'unité ou la sous-unité doit être identifiée

3.1.6
niveau de conception
niveau auquel les unités physiques et/ou fonctionnelles des éléments conçus lorsqu'ils existent déjà sont assignées dans la structure de décomposition du produit

NOTE Dans certains cas, «niveau de conception» est également appelé «niveau d'intervention».

3.1.7
exactitude de diagnostic
proportion de pannes, dans un dispositif, pouvant être correctement diagnostiquées dans des conditions données

3.1.8
tests pour diagnostic
procédure de tests réalisés dans le but d'établir un diagnostic

3.1.9
fausse alarme
indication de défaillance qui, après recherche des défaillances, n'est pas trouvée

3.1.10
taux de fausse alarme
le pourcentage de fausses alarmes sur le nombre total d'indications de défaillance

3.1.11
temps de détection de panne
durée écoulée entre l'instant de la défaillance et la détection de la panne

3.1.12
simulation de panne
introduction de pannes par des interventions non destructrices dans des unités matérielles et/ou, si nécessaire, la simulation via un logiciel afin de vérifier la capacité de diagnostic

3.1.13
fonction
performance exigée de l'entité

NOTE Une fonction est toujours associée, si elle est réalisée, avec une entité d'un niveau donné dans la structure de décomposition du produit.

3.1.14
modèle fonctionnel
représentation conceptuelle d'une entité décrivant les interrelations et dépendances entre ses terminaux de stimuli et de mesure (réponse)

NOTE Le modèle fonctionnel, qui est établi pendant le développement d'un produit, est en principe un diagramme de bloc montrant les fonctions du produit et auquel sont ajoutés les chemins de test envisagés par le responsable du développement.

3.1.15
vérification fonctionnelle
vérification de toutes les fonctions spécifiées des unités matérielles afin de prouver la capacité fonctionnelle

3.1.16
unité matérielle
élément de conception qui représente les fonctions et/ou sous-fonctions sous la forme matérielle, avec la possibilité d'inclure des composants logiciels

3.1.17
unité d'interchangeabilité
LRU
unité matérielle ou logicielle remplaçable qui peut être remplacée directement sur l'équipement par l'utilisateur ou par une structure de support de maintenance

3.1.18
concept de maintenance
interrelation entre les niveaux de conception et les niveaux de maintenance à appliquer pour la maintenance d'une entité

3.1.19
politique de maintenance
approche générale à la provision de maintenance et au support de maintenance basée sur les objectifs et les politiques des propriétaires, utilisateurs et clients

3.1.20
contrôle
supervision automatique des fonctions nécessaires au fonctionnement dans un mode opérationnel choisi, qui ne doit pas affecter le fonctionnement

3.1.21
contexte opérationnel
circonstances dans lesquelles une entité est supposée fonctionner

3.1.22
paramètre
quantité physique qui spécifie une fonction

3.1.23
produit
produit ou service spécifié

NOTE 1 Dans le contexte de la sûreté de fonctionnement, un produit peut être simple (par exemple un dispositif, un algorithme logiciel) ou complexe, par exemple un système ou un réseau intégré comprenant le matériel, le logiciel, les éléments humains, les activités et structures de support.

NOTE 2 Le produit a ses propres phases du cycle de vie.

NOTE 3 Le produit a la même définition qu'une entité.

3.1.24
structure de décomposition du produit
arbre hiérarchisé visualisant la composition physique d'un produit par assemblage des unités et sous-unités

3.1.25
unité d'interchangeabilité d'atelier
SRU
unité matérielle ou logicielle interchangeable qui peut être remplacée en atelier par l'utilisateur ou par la structure du support de maintenance au même niveau ou dans ses propres ateliers

3.1.26
signal
variation d'une quantité physique utilisée pour représenter des données

NOTE Un signal est représenté par un ou plusieurs paramètres.

3.1.27
spécification
définition détaillée des fonctions d'une entité pour un niveau donné de la structure de décomposition du produit

NOTE Il convient que les spécifications soient dérivées des exigences des systèmes et soient vérifiables.

3.1.28
définition de la prestation
SoW
document qui définit les marchandises et services à fournir

NOTE La définition de la prestation est préparée ou acceptée par le client et définit le travail pour lequel un contrat doit être placé et qui est fourni par l'entrepreneur. Cela constitue par conséquent le principal document technique suivant lequel les soumissionnaires présentent leurs offres, le fournisseur réalise le travail et le client accepte les marchandises et les services fournis.

3.1.29
stimulus
signal d'entrée avec des paramètres définis pour les besoins des fonctions de déclenchement

3.1.30
sous-fonction
sous-division d'une fonction (voir aussi fonction, 3.1.13)

3.1.31
terminal
terme générique pour désigner les points d'accès physiques aux signaux d'une entité à l'essai. Exemples de mise en application physiques ou de termes correspondants pour des expressions synonymes:

– broche

– connecteur
– connecteur de type enfichable
– point de test
– interface
– port

NOTE Un terminal est généralement identifié par un identifiant unique.

3.1.32
concept de test
description des résultats de l'analyse des exigences de testabilité du système et stipulation de la méthode consistant à savoir comment répondre aux exigences

3.1.33
couverture de test
rapport du nombre de fonctions défaillantes pouvant être diagnostiquées par une instruction de test donnée sur le nombre total de fonctions

3.1.34
équipement de test
outils (matériel et/ou logiciel) nécessaires pour la conduite des tests

NOTE Du fait de la technologie impliquée, ils sont divisés en matériel de test interne (ETI) et externe.

3.1.35
instruction de test
document décrivant comment les tests exigés dans les spécifications de test doivent être mis en œuvre

3.1.36
chemin de test
description de la mission des unités matérielles à leurs terminaux, prenant les étapes de test associées en considération

NOTE De plus, le chemin de test définit la relation (fonctionnelle) entre le stimulus et la réponse.

3.1.37
séquence de test
séries d'étapes de test

3.1.38
spécification de test
document dans lequel les séquences de test, paramètres et fonctions sont spécifiés

3.1.39
étape de test
plus petite unité dans un test mené sur un matériel

3.1.40
tâche de test
somme de tous les tests nécessaires pour répondre aux spécifications de la reconnaissance et localisation de panne

3.1.41
testabilité
caractéristique de conception qui détermine le degré jusqu'auquel un dispositif peut être testé dans des conditions données

3.2 Acronymes

AMDE(C) analyses des modes de défaillance, de leurs effets (et de leur criticité)
ATS système d'essai automatique (Automatic System Test)
CCV coût du cycle de vie
COTS produit sur étagère (Commercial Off-The-Shelf)
DP traitement des données (Data Processing)
EEA équipement de tests automatiques
ETI équipement de test intégré (Built-In Test Equipment)
FL localisation de panne (Fault Localization)
FM contrôle fonctionnel (Functional Monitoring)
FT vérification fonctionnelle (Functional Test)
FTA analyse par arbre de panne (Fault Tree Analysis)
HWE unité matérielle
LORA analyse du niveau de réparation (Level Of Repair Analysis)
LRU unité d'interchangeabilité (Line Replaceable Unit)
PCB carte imprimée (Printed Circuit Board)
RP reconnaissance de panne
SF sous-fonction
SoW définition de la prestation (Statement of Work)
SRU unité d'interchangeabilité d'atelier (Shop Replaceable Unit)
ST spécification technique
TI test intégré

4 Description de la testabilité et tests pour diagnostic

4.1 Généralités

Le fonctionnement et la maintenance efficaces et économiques d'un produit sont facilités par l'assurance que la testabilité est prise en compte pendant la conception et aussi pendant toutes les phases du cycle de vie. Les méthodes de test pour diagnostic applicables sont alors incorporées dans le produit comme composantes de la conception de la maintenance. La mise en application de la testabilité et les tests pour diagnostic sont accomplis tout au long du cycle de vie d'un produit.

Le coût du cycle de vie (CCV) est un aspect de plus en plus important pour l'évaluation de la qualité de toute conception. En supplément au coût d'acquisition immédiat, de nombreux clients demandent à contrôler les coûts associés à l'exploitation au quotidien, à la maintenance et à la logistique de maintenance. Ces coûts sont influencés au premier chef par la fiabilité, la maintenabilité du produit et les caractéristiques du support de maintenance. Dans ce contexte, l'application des techniques des tests pour diagnostic peut être un facteur significatif qui contribue à la réduction de certains éléments de coût du cycle de vie. Il convient que les contraintes résultant des efforts d'optimisation soient prises en compte lorsque les exigences des tests pour diagnostic sont établies.

Cette norme internationale est applicable à toutes les phases du cycle de vie, c'est-à-dire à partir du moment où le besoin pour un produit est identifié jusqu'aux phases de conception et de développement, à la phase de fabrication et d'installation et finalement à la phase d'exploitation et de maintenance comme suit (voir aussi Figure 1).

a) **Phase de conception et de développement**
Du concept à la réalisation du produit, il convient que les exigences affectées à un produit s'adaptent aux besoins spécifiques de son champ d'application, si nécessaire en passant par plusieurs pré-phases.

b) **Phase de fabrication et d'installation**
Pendant cette phase, il peut être nécessaire de vérifier les techniques de diagnostic en utilisant un matériel réel, et d'évaluer l'efficacité du produit. La documentation peut être préparée et la formation au personnel d'exploitation et de maintenance peut à présent intervenir.

c) **Phase d'exploitation et de maintenance**
Un changement dû à l'obsolescence peut apparaître sur un équipement testé. Il peut être nécessaire de poursuivre la fonction de test et il convient que le remplacement ou la mise à jour d'un équipement prenne en compte un besoin continu de test de diagnostic. Dans le dernier cas, il convient de réaliser une autre conception dans une nouvelle phase de développement.

En appliquant cette norme internationale, on présume que les pré-conditions sont remplies pour générer les données/Informations du produit nécessaires et que cela peut être vérifié et mis à jour durant tout le cycle de vie du produit.

L'Annexe B donne un exemple de développement de la testabilité, documenté et vérifié au regard de la conception du produit/système.

Les tests de diagnostic peuvent consister en ce qui suit:

– les tests de fonctionnement dans le but de vérifier qu'une fonction peut toujours être réalisée;

– le contrôle de condition qui est destiné à rechercher la condition de matériel qui se dégrade dans le temps;

Le contrôle de condition est étroitement lié aux concepts couverts par le test de diagnostic; il ne peut pas en être dissocié, et il ne convient pas qu'il le soit. Cependant, il n'est pas prévu qu'une couverture complète des aspects de pilotage de conditions soit assurée dans cette norme.

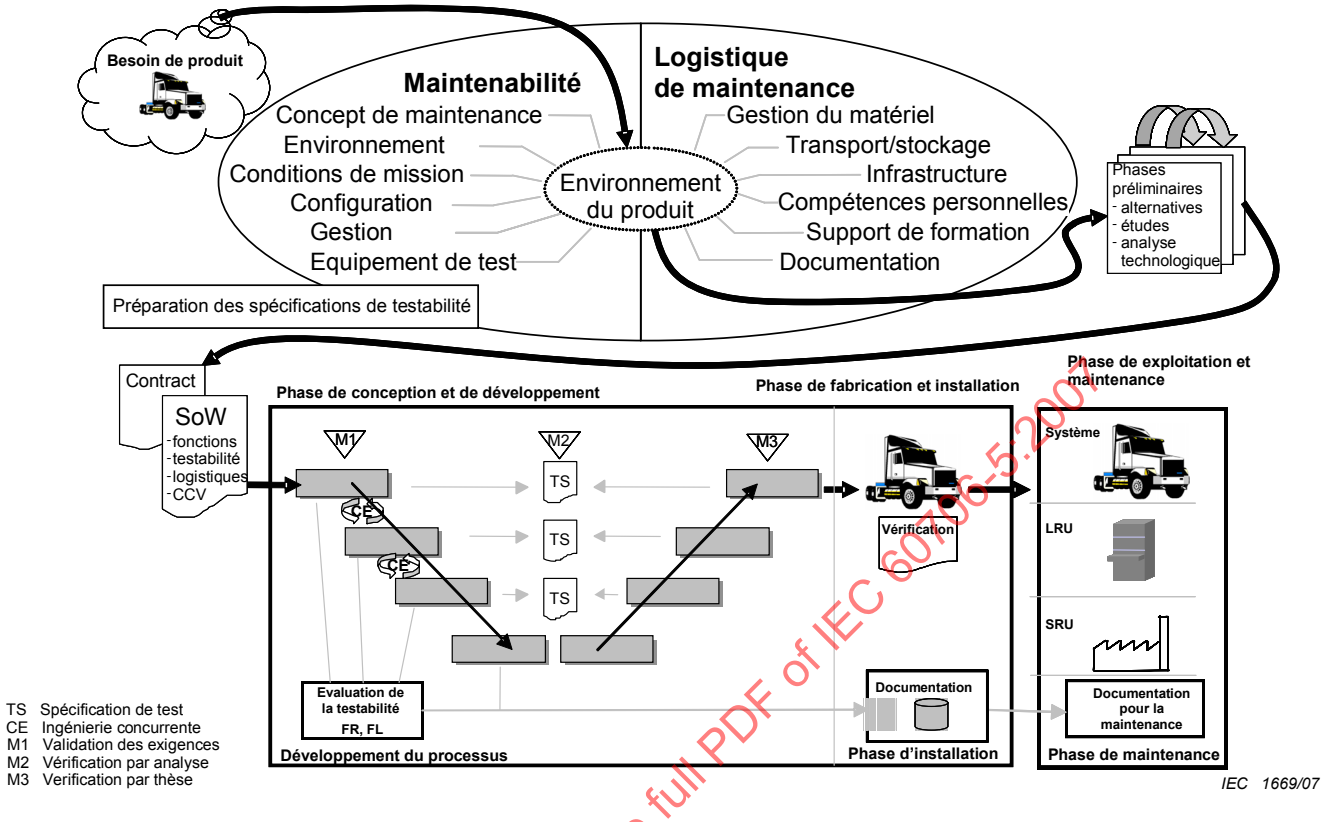


Figure 1 – Test de testabilité et de diagnostic pendant le cycle de vie

4.2 Objectifs de testabilité

La testabilité pendant la conception et le développement est étroitement alignée avec la maintenabilité, la disponibilité et la sécurité, et les objectifs principaux de testabilité sont traités par les questions suivantes pour chaque fonction du système.

a) Les défaillances de fonction peuvent-elles être détectées par un test de diagnostic ? Certaines fonctions ne peuvent pas complètement être soumises à essai à cause des contraintes de sécurité ou parce que l'essai est destructeur (tel que l'essai d'un mécanisme de survitesse sur un rotor).

b) Le test est-il pratique à réaliser ? La criticité de la défaillance de fonction, les coûts des tests (le coût de l'équipement de test, les coûts de maintenance de l'équipement de test de même que les coûts d'activité de test) et l'utilisation d'alternatives meilleures et moins chères peut conduire au constat qu'il n'est pas rentable de réaliser le test.

NOTE Pour les deux cas de a) et b), il convient que les méthodes alternatives soient adoptées pour assurer que la performance de ces fonctions est maintenue pendant la vie du produit. Ensemble, ces éléments contribuent à la couverture de test. Une valeur basse de couverture de test peut être préjudiciable du fait de l'impossibilité de soumettre le système à un test pour confirmer la performance opérationnelle pendant son cycle de vie, mais il indique aussi que la capacité de maintenabilité et de maintenance est telle que les tests sont nécessaires.

c) A quels stades de son cycle de vie une entité doit elle être testée? Il convient de considérer l'aptitude aux tests pour chaque étape du cycle de vie; effectuer un test sur une fonction au niveau unité peut être possible mais impraticable au niveau système. On peut l'expliquer par un exemple: considérons une machine à laver et sa fonction d'évacuation de l'eau résiduelle. Il serait utile, d'un point de vue utilisateur, de mener un test à l'étape de pré-fonctionnement pour confirmer que la fonction peut être réalisée avant la mise en marche (réaliser un test à l'étape opérationnelle apporterait peu de bénéfice). La conception pour cette fonction peut ne pas nécessiter l'introduction d'équipement de test pour réaliser des tests sur cette fonction car

   1) la vie d'une pompe et de l'équipement associé dépasse largement la vie du produit (d'autres défaillances et le coût de leur réparation peut définir la vie du produit);

2) la tâche de maintenance pour retirer un blocage possible peut être facilement accommodée;

3) les unités qui réalisent cette fonction peuvent être complètement soumises à des tests à l'étape d'unité et à l'étape au niveau du système avant la livraison;

4) déterminer les étapes à tester peut également influencer le coût du cycle de vie.

d) Jusqu'à quel stade convient-il de pousser les tests ? Le niveau des tests est également un critère important et, comme dans l'exemple ci-dessus, il est étroitement en ligne avec le concept de maintenance. Le niveau de test spécifie le niveau auquel l'unité ou sous-unité doit être identifiée. Par exemple, un test système peut identifier l'unité à remplacer, mais peut également identifier la sous-unité qui a besoin d'être remplacée avec peu ou pas d'impact sur le coût. Cela peut limiter les coûts associés à l'équipement de test nécessaire au niveau unité pour identifier et remplacer la sous-unité défectueuse.

Il s'agit d'un principe de base dans la conception de la testabilité que toutes les fonctions soient vérifiables. Il convient, cependant, de noter que la couverture de test de 100% n'est pas nécessairement souhaitable, les tests pouvant créer des défaillances qui se manifestent pendant le fonctionnement, ce qui peut être pire que de ne pas en faire du tout, par exemple de réelles défaillances introduites par des tests ou de fausses alarmes. De la même façon, une couverture de test de 100% n'est pas recommandée pour toutes les questions de sécurité, le test lui-même pouvant porter préjudice à la sécurité du système. Il est plus important que les tests donnent une confiance substantielle dans le fonctionnement du système. Pour obtenir cela, il convient que les écarts de la couverture de test de 100% soient toujours absolument justifiés.

Néanmoins, il convient que les objectifs de testabilité ne contredisent pas les objectifs plus importants, par exemple la disponibilité.

e) Comment faut-il gérer les fausses alarmes et les pannes non détectées? Le test système peut détecter et rendre compte d'une défaillance à l'utilisateur lorsqu'une défaillance n'existe pas vraiment. Cela peut entraîner des recherches qui ne sont pas nécessaires et avoir pour conséquence le report d'une fausse alarme. Cela peut également entraîner une action de maintenance non nécessaire qui se conclut par un diagnostic de «pas de panne». Il convient que les taux de fausse alarme pour les diverses résolutions ne dépassent pas les critères définis et, lorsque c'est possible, soient réduit à zéro. Les méthodes qui sont reconnues pour minimiser ces occurrences peuvent impliquer des systèmes de retour qui évaluent constamment l'environnement et se re-calibrent eux-mêmes pour permettre la dégradation du composant dans des critères définis. La répétition d'un essai pour éliminer une fausse alarme (le scénario de l'essai peut avoir changé suffisamment pour que l'alarme ne se déclenche pas) augmentera le temps d'essai et il convient qu'il soit évité.

   Des pannes peuvent être indiquées quand aucune panne n'existe. Cela peut être dû à plusieurs raisons:

   1) si un défaut est trouvé dans le système et que le diagnostic identifie l'élément défectueux, mais qu'aucun défaut ne peut être identifié après retrait de l'élément et des tests indépendants, il faudra alors vérifier les spécifications d'essai du système en relation avec les spécifications d'essai de l'élément défectueux;
   2) mauvais diagnostics (l'essai n'identifie pas la partie défectueuse de façon adéquate);
   3) difficultés d'interface (par exemple, un connecteur défectueux a entraîné le retrait d'une unité et une reconnexion supprime la défaillance);
   4) mauvais matériel d'essai comprenant ETI (par exemple une défaillance détectée n'existe pas);
   5) panne intermittente (des unités à risque peuvent parfois contenir des défauts qui ne sont pas évidents sauf dans certaines circonstances);
   6) les problèmes de niveau de tolérance de la conception (une défaillance dans le système d'essai peut ne pas être enregistrée comme défaillance dans l'unité d'essai). Les unités à risque peuvent avoir des valeurs extrêmes dans la bande de tolérance qui résultent en un rejet continuel;
   7) défauts logiciels (défauts apparaissant durant utilisation qui ne sont pas correctement testés);
   8) des difficultés pour l'utilisateur et l'«opérateur de maintenance» (formation inadéquate, rapidité des délais, manques de pièces détachées) peuvent tous mener au rejet de bonnes unités.

   Tous les symptômes décrits ci-dessus peuvent avoir un effet néfaste en fonctionnement et support et il convient de les éliminer ou de les minimiser quand cela est possible;

f) Les essais de systèmes peuvent-ils être adaptés ? Les essais de systèmes sont impliqués dans l'assurance qu'un système fonctionnera correctement pour des entrées définies et dans un environnement défini. Les exigences de testabilité et la capacité de localiser un défaut ne dictent pas nécessairement la procédure d'essai. Mettre à l'essai une fonction d'ensemble, avec des essais consécutifs plus poussés si nécessaire, peut engendrer une économie de temps substantielle et une forte amélioration de la convivialité pour l'utilisateur. L'utilisation d'outils tels que la FMECA (voir Annexe B) et FTA peut aider à définir la séquence de niveaux inférieurs en déterminant quelle fonction aura le plus probablement eu une défaillance

4.3 Objectifs des tests pour diagnostic

L'objectif des tests pour diagnostic est de fournir la méthode la plus efficace vis-à-vis des coûts, la plus rapide et la moins ambiguë concernant l'identification de panne à un niveau déterminé par le concept de maintenance de l'équipement en test. De bons tests pour diagnostic vont

- augmenter la disponibilité de l'équipement;
- diminuer les coûts de maintenance;
- réduire le risque de dommages indirects;

- améliorer la sécurité du système;
- optimiser l'utilisation opérationnelle.

Pour atteindre leur objectif, il convient que les tests pour diagnostic

- fournissent des types de vérifications de confiance afin de confirmer l'aptitude au service de l'équipement concernant le rôle qui lui est dévolu;
- reconnaissent les défaillances catastrophiques et les dégradations;
- localisent les pannes en rapport avec la fonction défaillante ou LRU défaillante;
- avertissent des défaillances d'usure potentielle grâce à une évaluation des états d'usure;
- fournissent des données pour la maintenance et l'exploitation de l'équipement.

Les principales applications des dispositifs de tests de diagnostic sont

- les vérifications fonctionnelles et de sécurité avant la mise en fonctionnement du système;
- le contrôle des performances en fonctionnement;
- l'identification des défaillances du système en environnement opérationnel, au niveau de l'ensemble défaillant ou de la LRU;
- la localisation détaillée des pannes dans les ateliers de réparation.

4.4 Méthodes utilisées pour les tests de diagnostic

Les procédures possibles pouvant être appliquées pour les essais de diagnostic vont des mesures purement manuelles et de l'évaluation des caractéristiques mécaniques au diagnostic entièrement automatisé de processus et installations complètes, y compris le test de composants élémentaires et de systèmes complexes. La large panoplie de méthodes de diagnostic appliquées se classe en deux catégories principales:

– le diagnostic externe utilise des équipements de test distincts du produit qui ne sont branchés que lorsque c'est nécessaire. L'équipement de test utilisé peut être d'une nature très générale, adapté aux buts requis à partir d'appareils standards, ou bien être spécialement conçu pour l'équipement à essayer. Des EEA pilotés par ordinateur peuvent également être utilisés;

– le diagnostic interne utilise en permanence l'équipement de test intégré (ETI) qui peut être mis en fonctionnement de façon continue ou intermittente pendant le fonctionnement du système. En outre, des tests spéciaux, pour un état de fonctionnement réduit du système, ou bien hors fonctionnement, peuvent aussi être réalisés.

4.5 Méthodes utilisées pour le pilotage des conditions

En plus des tests pour diagnostic qui servent pour les pannes discrètes, de nombreux produits bénéficient aussi du pilotage de condition. Cela est réalisé comme une partie de la maintenance préventive pour surveiller la dégradation des conditions et performances.

Les méthodes utilisées pour le pilotage des conditions peut varier avec le type d'équipement et peut inclure ce qui suit:

– analyse des vibrations;
– analyse de fluides/lubrifiants;
– détection ultrasonique;
– thermographie;
– alarmes et arrêts intégrés dans le système de contrôle.

4.6 Concept de testabilité

La testabilité est la caractéristique de conception d'un produit qui garantit que les capacités fonctionnelles de cette unité peuvent être évaluées en temps voulu et de façon efficace et que

les pannes peuvent être reconnues et, si nécessaire, localisées. Assurer la maintenabilité d'un produit est un des premiers composants.

Le test de diagnostic est l'action de maintenance résultante qui survient comme partie de la maintenance préventive telle que décrit dans le concept de maintenance. La couverture de test est le degré auquel le test de diagnostic peut être appliqué. Le test de diagnostic est constitué de deux étapes: la reconnaissance de panne (RP) et la localisation de panne (FL). La reconnaissance de panne identifie si une panne existe et la localisation de panne détermine la nature spécifique de cette panne.

Il convient que le test de diagnostic prenne également en considération les chaînes de tolérance. Pour un paramètre particulier, il y a généralement une limite supérieure et une limite inférieure qui délimite la zone de réussite ou d'échec. Une fonction d'unité peut avoir des limites serrées, mais lors de l'intégration de l'unité, ces limites sont modifiées par la variabilité des autres unités qui contribuent à la fonction finale du système. En plus des chaînes de tolérance, il convient de prendre en considération la précision de l'équipement réalisant les tests, avant que la bande de tolérance réussite/échec réelle soit définie pour un test particulier. Les résultats des tests rassemblés pendant le développement fournissent une estimation de la largeur du procédé (la sommation de la production de fonction et la précision de l'équipement de test, comprenant la précision des stimuli de l'équipement de test de même que la précision de lecture des dispositifs de mesure). Cependant, il n'est pas prévu qu'une couverture complète des aspects de pilotage de conditions soit assurée dans cette norme.

Les spécifications relatives à la fonctionnalité, comprenant la testabilité, sous la forme de valeur caractéristique pour la qualité de la reconnaissance de panne et la localisation de panne ont un impact direct sur les caractéristiques fonctionnelles de base du produit. Si la règle "il convient que les fonctions qui sont développées puissent être vérifiées par des paramètres " est suivie, alors la reconnaissance de panne et la localisation de panne sont développées simultanément depuis le début comme partie intégrante de la fonctionnalité. De cette manière, le coût d'un produit restera dans les limites prescrites. Si des éléments de la reconnaissance de panne et de la localisation de panne sont intégrés ultérieurement, cela mènera non seulement à des délais considérables mais aussi à un produit de qualité réduite avec des coûts extrêmement élevés d'action de reprise/correction.

5 Spécification de testabilité

5.1 Généralités

Des dispositions appropriées et contractuelles sont un préalable essentiel à la conversion des exigences de tests de diagnostic en réalisations pratiques mesurables. Pour rendre possible une conception optimale, un développement et une fourniture de procédures pour des tests de diagnostic, il convient que le client fournisse une spécification précise de ses exigences et contraintes de testabilité. Pour cela, il convient que le client procure au fournisseur les documents suivants:

– une définition de la prestation (SoW). Ce document contient toutes les exigences fonctionnelles relatives aux tests. Dans ce document, le client spécifie toutes les fonctions/fonctionnalités, y compris la testabilité;

– une spécification de testabilité. Dans ce document, le contractant (responsable du développement) détermine les besoins (matériel, logiciel) pour réaliser les fonctions d'ingénierie opérationnelles et de test et les caractéristiques de performance exigées par la définition de la prestation (SoW).

5.2 Définition de la prestation

La définition des exigences est constituée de descriptions détaillées des besoins du client et a pour but de constituer la base du programme de conception et de développement. La mise à jour est possible si des informations supplémentaires deviennent disponibles en cours de développement. Cependant, il convient que les modifications soient mutuellement avalisées du fait qu'elles induiront souvent des délais supplémentaires et des pénalités en coût. Il convient que les exigences comprennent ce qui suit:

– les objectifs des tests pour diagnostic (voir 4.3),
– le concept d'exploitation (voir 5.3 et Tableau 1),
– le concept de maintenance (voir 5.3 et Tableau 2),
– une description qualitative de l'environnement économique (voir 4.1);
– les méthodes et solutions préférentielles (voir 4.4).

5.3 Spécification

La spécification de testabilité détermine les exigences relatives au produit, et éventuellement pour la phase de développement. Il convient que les spécifications de testabilité définissent chacune des étapes de test et des éléments de fonction associés pour lesquels les spécifications de test sont applicables. Il convient que ces dernières comprennent ce qui suit.

a) Les tâches et les applications des tests pour diagnostic:
   1) une liste des pannes concernant la sécurité pour lesquelles un degré de détection de pannes aussi proche que possible de 100 % est requis;
   2) une liste des pannes critiques pour laquelle une couverture de test de 100% est nécessaire ou des preuves pour justifier que les tests peuvent être omis;
   3) une limite inférieure de couverture de test pour toutes les autres fonctions ou une couverture de test globale pour toutes les fonctions (les fonctions à utiliser pour la couverture de test doivent être déterminées);
   4) une valeur maximale du temps de détection de pannes;
   5) des valeurs objectifs (maximum) des temps de localisation de panne;
   6) un objectif et une valeur minimale pour l'exactitude de diagnostic;
   7) la valeur maximale du taux de fausse alarme;
b) Il convient que la conception pour la testabilité comprenne ce qui suit:
   1) les exigences générales;
   2) les exigences détaillées au moyen de listes de vérification;
   3) les critères de conception concernant la testabilité;
c) Les temps et procédures pour ce qui suit:
   1) la vérification de la testabilité;
   2) la vérification de la sécurité.

Il convient que les conséquences du non-respect des exigences spécifiées selon les éléments ci-dessus soient définies.

Les tâches d'essai qu'il convient de spécifier sont décrites plus en détails en 5.4.3. A ce stade, il convient d'identifier le besoin d'une évaluation de méthodes alternatives (voir 5.6).

Les activités de tests de diagnostic sont étroitement interconnectées avec les processus d'exploitation et de maintenance du produit. Par conséquent, les concepts opérationnels et de maintenance sont des facteurs importants à considérer au moment d'établir des exigences de tests pour diagnostic. Il convient de définir les deux dès que possible dans le cycle de vie du système, de préférence dans la phase de concept et définition. Il convient que le concept d'exploitation soit le premier pris en considération afin que le système satisfasse correctement

à ses exigences. Il convient que le concept de maintenance soit élaboré afin de permettre de satisfaire aux besoins opérationnels avec l'utilisation la plus efficace possible des ressources pour un coût minimal. Un certain degré de compromis devra invariablement être pris en compte afin de réaliser l'équilibre optimal parmi des exigences qui peuvent parfois être contradictoires.

Les éléments qu'il convient de prendre en considération pour définir le concept d'exploitation sont indiqués dans le Tableau 1. Chacun d'eux nécessite d'être spécifié en détail de sorte que l'environnement de maintenance ainsi que les contraintes d'exploitation puissent être correctement pris en compte.

Le concept de maintenance détermine les tâches de test à appliquer au niveau de conception correct, le personnel pour le réaliser et l'équipement de test à utiliser. Il convient de prendre en compte les besoins de tous les éléments impliqués dans le produit (développement, production, exploitation et maintenance). Le Tableau 2 contient une liste des éléments du concept de maintenance à considérer.

Tableau 1 – Eléments du concept d'exploitation

Elément	Possibilités		
Situation	Mobile		
	Fixe	Transportable	Lieu variable
			Lieu fixe
		Non transportable	
Mode de fonctionnement	Fonctionnement continu	Contrôle permanent	
		Contrôles à certains moments dans le temps	
		Arrêts autorisés et conditions d'arrêt	
	Fonctionnement intermittent incluant les conditions d'intermittence		
Conditions de contraintes en exploitation	Fonctionnement sous contraintes réduites		
	Fonctionnement sous contraintes nominales		
	Fonctionnement sous contraintes élevées		
Conséquences	Sécurité		
	Coût	Utilisation réduite	
		Dommages indirects	
		Coûts de maintenance	
	Mesures correctives d'urgence		
Conditions d'environnement	Contraintes mécaniques		
	Contraintes thermiques		
	Contraintes électriques		
	Contraintes chimiques		
	Autres		
Personnel	Non formé		
	Formé dans un domaine différent		
	Formé	Qualification élevée	
		Qualification moyenne	
		Qualification faible	
Manipulation	Manuelle		
	Partiellement automatisée		
	Complètement automatisée		

Tableau 2 – Eléments du concept de maintenance

Elément	Détails nécessaires		
Tâches de maintenance	Préventive	Maintenance	
		Essai de diagnostic	
		Réparation programmée	
	Corrective	Niveau système	Détection de panne
			Localisation de panne
			Réparation (remplacement)
			Etalonnage
			Vérification fonctionnelle
		Niveau composant	Localisation de panne
			Réparation
			Etalonnage
			Vérification fonctionnelle
Temps de maintenance	Contrôle permanent		
	Maintenance préventive	Intervalles	Période de temps
			Action
		Types	Niveau
			Maintenance hors fonctionnement
			Maintenance en fonctionnement
	Maintenance corrective		
Lieu de maintenance	Fixe	Nombre d'ateliers	
		Répartition géographique des ateliers	
		Potentiel technique des ateliers	
	Mobile	Equipement de station	
		Potentiel technique de la station	
Procédure de maintenance	Procédure		
	Ressources	Matériel	
		Logiciel	
	Documentation (descriptive, illustrative) pour		Matériel
			Logiciel
Support de maintenance	Stocks	Nombre de magasins	
		Répartition géographique des magasins	
		Taille des stocks	
		Conditions de stockage	
	Gestion des stocks	Approvisionnement	
		Fourniture	
		Transport	
Environnement de maintenance	Conditions thermiques		
	Autres conditions		
Personnel de maintenance	Formation de base	Type de formation	
		Niveau de qualification	
	Formation spéciale	Niveau système	
		Niveau composant	
	Formation de remise à niveau	Intervalles	
		Contenu	

5.4 Caractéristiques de testabilité

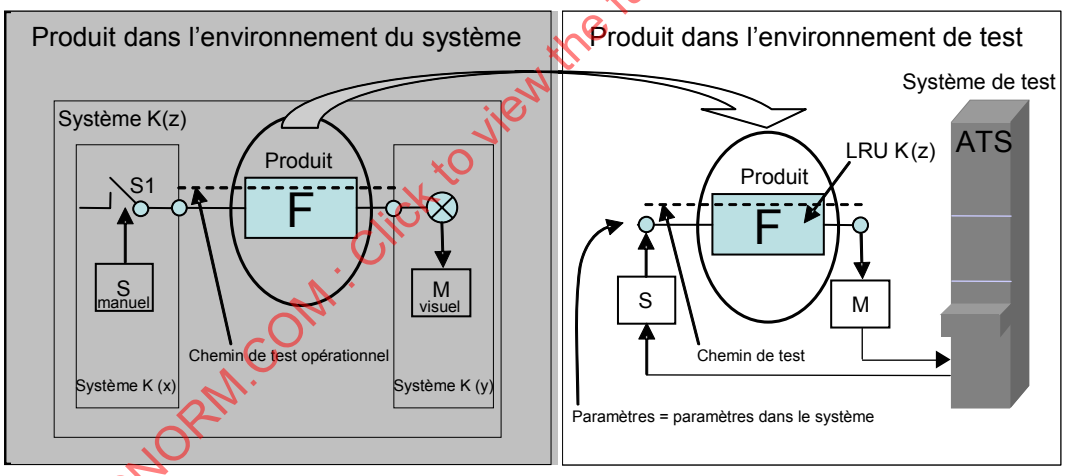
5.4.1 Eléments de testabilité

Les éléments de testabilité peuvent être caractérisés par les paramètres suivants (les expressions mathématiques sont données à l'Annexe A):

– reconnaissance de panne: voir CEI 60050-191;
– temps de détection de panne: voir 3.1.11;
– localisation de panne: voir CEI 60050-191;
– temps de localisation de panne: voir CEI 60050-191;
– exactitude de diagnostic: voir 3.1.7;
– couverture de test: voir 3.1.33;
– taux de fausse alarme: voir 3.1.10.

5.4.2 Contexte opérationnel

Un produit peut être utilisé dans différents environnements, selon les exigences placées sur ce produit dans la définition du travail. En ce qui concerne la testabilité, une distinction est faite entre l'environnement du système (condition d'exploitation) au niveau de conception stipulé, comme montré dans la Figure 2, et l'environnement de test correspondant aux conditions de maintenance exigées. Dans ce dernier cas, le produit fonctionne dans une simulation de système/produit. Ici, il convient que tous les paramètres réglés pour les tests sur le matériel correspondent à ceux du système. La Figure 2 montre comment l'un est relié à l'autre.



Légende

S Stimulus
M Mesure
F Fonction
K(x),K(y),K(z) Systèmes (entités) faisant partie de la décomposition du produit

IEC 1670/07

Figure 2 – Contexte opérationnel

5.4.3 Tâches de test

5.4.3.1 Chemins de test

La plus petite unité d'un test comprend un chemin de test qui commence avec au moins un stimulus, passe par une fonction/sous-fonction et se termine avec le minimum d'une mesure comprenant une comparaison avec une valeur spécifiée.

Les chemins de test nécessaires à la reconnaissance de panne passent par toutes fonctions d'une chaîne d'unités remplaçables.

Il convient que les chemins de test nécessaires pour la localisation de panne consistent en tests sur des interfaces physiques entre unités remplaçables.

La tâche de test comprend la reconnaissance et la localisation de panne et est menée dans les portions A + B + C + D = 100 % comme montré au Tableau 3.

Tableau 3 – Tâche de test

Portion	Tâches de test	Exemple *RP* valeurs spécifiées	Exemple *FL* valeurs spécifiées
A	Tests pendant le fonctionnement (tests en ligne)	50 %	0 %
B	Tests en conditions de test, sans équipement de test externe (tests hors ligne)	50 %	95 %
C	Tests en conditions de test, avec équipement de test externe	0 %	5 %
D	Non testable	0 %	0 %

Tous les tests listés au Tableau 3 sont disponibles pour la localisation de panne. La localisation d'unités matérielles remplaçables défectueuses (LRU/SRU) est obtenue à partir d'informations contenues dans les résultats de test des séries de test qui couvrent différents chemins de test traversant le LRU/SRU. Le modèle fonctionnel (voir Annexe B) fournit les informations nécessaires. Dans cet exemple, il y a uniquement la couverture de test pour *RP* dans les portions A et B et *FL* dans les portions B et C.

Il convient que la conception du produit donne des caractéristiques permettant de mener toutes les tâches de test en accord avec les exigences indiquées dans le SoW. Ces caractéristiques sont sous-divisées en caractéristique TI et, quand cela est permis, en équipement de test externe avec les entrées de test nécessaires.

5.4.3.2 Test intégré

TI est une caractéristique du produit ayant pour but la réalisation des tests. Une fonction TI est constituée au moins d'un stimulus, un chemin de test par une fonction/sous fonction et au moins une mesure comprenant une comparaison avec la valeur spécifiée. Le nombre de fonctions TI nécessaires est dérivé des exigences données dans le SoW et dépend des valeurs spécifiées exposées pour la reconnaissance de panne. TI consiste en portions matérielles et logicielles.

NOTE Dans l'équipement électronique, la détection de défaillances peut souvent être obtenue simplement par la surveillance de certains paramètres vitaux, par exemple les tensions d'alimentation, la puissance ou fréquence de forme de signaux bien définis, les identités des signaux discrets ou les sommes de contrôle de données. Ce sont des formes spécialisées de TI en ligne où aucun stimulus supplémentaire n'est appliqué. En revanche, par l'ETI, des signaux de référence supplémentaires sont générés pour permettre au TI de les comparer avec les valeurs nécessaires.

Les tests ETI font partie de tous les tests fonctionnels menés sur un produit et sont divisés en tests en ligne et hors ligne.

Les tests en ligne sont ceux qui sont menés en continu pendant le fonctionnement d'un produit.

Le fonctionnement doit être interrompu avant que les tests hors ligne ne puissent être réalisés. Il convient généralement de n'utiliser de tels tests que pour la localisation de panne.

5.4.3.3 Tests au moyen de l'équipement de test externe

Si l'équipement de test externe est nécessaire et est autorisé par le SoW, alors on accède au produit par les entrées de test (par exemple connecteurs de test). L'équipement de test externe travaille sur le même principe que les fonctions ETI et par conséquent nécessite des

chemins de test de stimuli, par la fonction au test au travers de point de mesure, incluant l'évaluation de résultat de test.

5.5 Valeurs caractéristiques pour évaluer la testabilité

Pour obtenir une évaluation uniforme de la testabilité pour tous les utilisateurs de cette norme, il est nécessaire d'introduire des valeurs caractéristiques pour les composants de testabilité (*RP*, *FL* et couverture de test). Ces valeurs sont neutres au regard du produit, elles reflètent la performance nécessaire du produit testable et sont comparables pour tous les utilisateurs de cette norme.

Il convient que les valeurs caractéristiques soient spécifiées en avance dans le SoW. Elles sont le point de référence pour l'évaluation de la testabilité. En spécifiant les valeurs caractéristiques, il convient de prendre en compte le concept de maintenance, l'effort d'ingénierie et les coûts associés. Si les exigences sont déjà disponibles pour l'ingénieur du développement, alors il convient qu'il évalue la vérification de testabilité et la vérification de sécurité.

Il convient que les conséquences du non-respect des exigences spécifiées selon les éléments ci-dessus soient définies.

5.6 Critères pour l'évaluation de conceptions de diagnostic alternatives

Il convient de comparer et évaluer les conceptions de diagnostic alternatives possibles afin de choisir la solution optimale. Il convient que les critères économiques suivants soient pris en compte.

a) Les coûts d'investissement sont constitués de ce qui suit:
   1) nombre de systèmes nécessaires, basé sur l'utilisation et la disponibilité;
   2) coûts de développement;
   3) coûts de logiciels non répétitifs;
   4) coûts des installations de maintenance.
b) Les coûts unitaires d'équipement dépendant de
   1) la complexité;
   2) la quantité à produire;
   3) le degré de redondance;
   4) le degré de la capacité en TI;
   5) le standard de qualité.
c) Les coûts relatifs à la maintenance sont constitués de ce qui suit:
   1) coût de maintenance préventive et corrective;
   2) gain résultant d'un système de diagnostic évitant des détériorations conséquentes;
   3) degré d'automatisation comparé aux niveaux de formation;
   4) durée de vie prévue pour l'équipement.
d) Moyens d'augmenter les bénéfices en exploitation:
   1) caractéristiques de manipulation améliorées;
   2) disponibilité améliorée, par exemple grâce à des diagnostics et à des réparations rapides des pannes, ou bien par utilisation de la redondance;
   3) utilisation accrue.
e) Les autres facteurs comprenant ce qui suit:
   1) potentiel de modification;
   2) incidence technique et économique de matériel ou de logiciel supplémentaire sur la sécurité et la fiabilité de l'équipement;

3) capacité à détecter des défaillances transitoires et intermittentes;
4) capacité du système de diagnostic pour un mode réversible;
5) gains de rendement de coût utilisant ETI comparés à l'équipement de test externe;
6) Utilisation de COTS.

6 Testabilité dans le processus de développement

6.1 Généralités

Une fois toutes les exigences de la sphère d'exploitation du produit déterminées, alors le développement du produit peut commencer.

Le développement réussi d'un produit est premièrement basé sur des instructions uniformément définies sur la façon de procéder. Cela permet une compréhension commune des exigences relatives au développement, à la mise à jour et à la modification d'un produit par toutes les parties impliquées. Cela s'applique également aux activités d'accompagnement telles que l'assurance qualité, la gestion de la configuration et la gestion de projet technique.

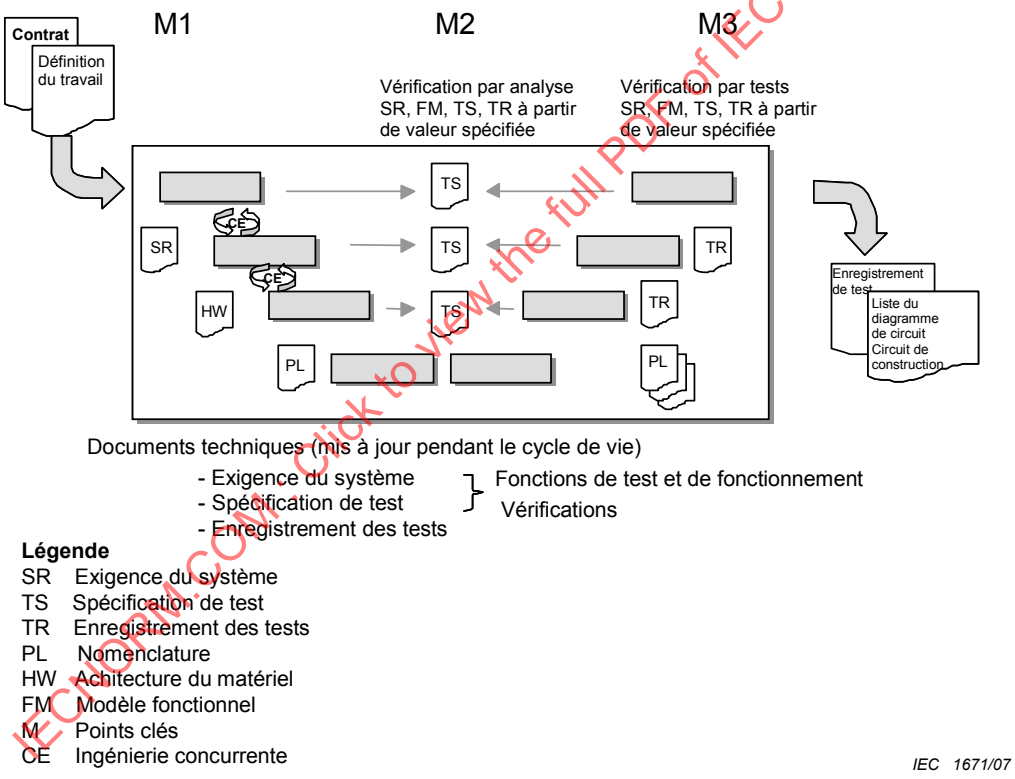


Figure 3 – Processus de développement conforme au modèle en V

Il convient que trois points clés soient décrits en développant des produits testables:

– M1 – début du développement par le contractant avec la validation des exigences;
– M2 – preuve théorique de la testabilité du produit, avec vérification par l'analyse;
– M3 – démonstration pratique de la testabilité du produit, avec vérification par les tests.

La Figure 3 montre comment ceux-ci sont liés au processus de développement dans le modèle en V.

Les étapes suivantes sont nécessaires pour aboutir à un produit testable:

– exigences de vérification en terme d'exhaustivité et, si nécessaire, requête pour que le client fournisse les exigences manquantes;
– mener une analyse d'exigences pour générer une spécification;
– assigner le produit aux niveaux de conception prescrits par le client;
– réaliser une conception fonctionnelle (fonctions/sous-fonctions et les relier);
– réaliser une conception d'ingénierie (attribution matériel);
– développer la reconnaissance de panne et optimiser si nécessaire;
– développer la localisation de panne et optimiser si nécessaire;
– préparer les activités de vérification;
– effectuer les vérifications;
– documenter la vérification.

Dès que les unités matérielles ont été définies dans le projet de développement, ces unités déclenchent un nouveau processus à un niveau de conception plus profond en accord avec la description de tâches prescrite. Si certaines fonctionnalités ne peuvent pas être réalisées au moyen d'unité matérielle définie, alors un processus d'amélioration itératif est commencé par lequel les spécifications modifiées se déroulent au niveau précédent et la nouvelle unité matérielle est définie. Une fois toutes les unités matérielles définies jusqu'aux composants individuels, le processus d'intégration peut commencer dans la description des tâches.

L'application de normes et d'outils informatiques associés facilite considérablement le développement.

6.2 Attribution fonctionnelle

Le processus de développement de testabilité est basé sur l'exigence que toutes les fonctions et sous-fonctions contenues dans le produit devraient être vérifiables. Cela est obtenu par une allocation adéquate des étapes de test des unités matérielles et sous-fonctions associées.

Une procédure appropriée pour la mise en œuvre de l'exigence de testabilité est décrite dans l'Annexe B. C'est une sorte de méthode AMPE basée uniquement sur un modèle fonctionnel.

6.3 Ingénierie de testabilité

6.3.1 Critères de conception concernant la testabilité

Le but de cette partie du programme est de définir les moyens de satisfaire aux exigences des tests pour diagnostic établies pour le produit. Il s'agit d'une partie de la maintenabilité pendant la conception qui est couverte par la CEI 60300-3-10 et la CEI 60706-2. Dans ce contexte, il convient de prendre en considération les critères suivants de conception de testabilité:

– partition fonctionnelle en groupes et unités fonctionnels avec des interfaces clairement disposées et bien définies. Chaque fois que possible, il convient que les partitions physiques et électriques soient compatibles avec cette structure afin de faciliter un ajustement optimal des diagnostics, de la maintenance et de la logistique;
– préférence pour l'utilisation de fonctions, composants et éléments de conception, pour lesquels l'état et le comportement transitoire peuvent être mesurés et évalués facilement par des procédures de test de diagnostic simples et appropriées;
– prise en considération des procédures de mesure qui sont applicables durant la maintenance et compatibles avec l'équipement externe existant ou prévu. Il convient que l'accessibilité physique et électrique des équipements de mesure soit également prise en compte;
– il convient que l'extension d'autotest soit cohérente avec le niveau d'analyse de réparation (LORA) comme décrit dans la CEI 60300-3-10;
– il convient que les points de test soient fournis et étiquetés de façon adéquate, particulièrement ceux exigés pour l'équipement de test externe;

– il convient que les définitions de défaillance et les critères de points soient bien définis avant de finaliser les critères de testabilité du produit;

– initialisation: il convient que le système ou l'équipement soit conçu de telle sorte qu'il ait un état initial bien défini afin de commencer le processus de localisation de panne. En cas de défaillance, il convient que l'initialisation se produise automatiquement et de manière répétée;

– il convient que l'application de procédure de test et de stimulations externes n'ait aucun effet dommageable, ni sur les composants eux-mêmes ni sur l'équipement considéré ou le système global;

– il convient que tous les systèmes de bus soient accessibles pour les mesures;

– il convient que le logiciel fonctionnel et, si possible, le logiciel d'application de diagnostic soient conçus et documentés de sorte qu'ils puissent être facilement vérifiés par le personnel de maintenance.

6.3.2 Conception pour la testabilité

Une fois la décision sur le choix des fonctions à réaliser dans les unités matérielles a été prise, il convient que ces unités matérielles soient attribuées aux niveaux de conception du produit. Cette décomposition est hiérarchique (du haut vers le bas). Le nombre de niveaux dépend de la complexité du produit/système et de sa conception technique. Pour des besoins de simplification/standardisation, on donne une classification ascendante aux niveaux de conception individuelle du composant vers le système (K1…Kn). Des niveaux de systèmes plus élevés peuvent être introduits, mais ne reçoivent qu'une numérotation consécutive (par exemple système 4, système 5, etc.).

Dans le cadre de la conception d'ingénierie, les fonctions/sous-fonctions sont attribuées aux unités matérielles. Ici, une attention particulière est à porter à ce qui suit:

a) nombre minimal d'interfaces (où les sous-fonctions sont séparées);

b) groupement fonctionnel (combinaison de SF avec la fonction de niveau le plus haut associée;

c) n'utiliser que des interfaces normalisées (par exemple Bus). Si nécessaire introduire un bus de test séparé.

Il convient que la conception pour la testabilité incorpore les étapes de test diverses impliquées dans la vie du système. Cela comprend ce qui suit:

1) la phase de production;

2) la phase de stockage;

3) la phase de pré-exploitation;

4) la phase d'exploitation;

5) la phase de post-exploitation;

6) les étapes de maintenance; et

7) la phase de mise au rebut.

Il convient de traiter chaque étape séparément et collectivement pour obtenir une solution efficace vis-à-vis du coût pour la testabilité d'un produit. Il convient également de considérer que certains systèmes exploitent de multiples rôles et peuvent être utilisés dans différents scénarios, activant différents éléments fonctionnels, et il convient de traiter ces éléments de façon similaire.

6.3.3 Utilisation des produits sur étagère (COTS)

Une pré-condition pour l'utilisation des produits COTS est qu'ils répondent aux exigences indiquées dans le SoW et, par conséquent, à tous les besoins relatifs à la sphère d'exploitation, comprenant la testabilité, la maintenance et la disponibilité de la documentation nécessaire pour la phase en-service. Dans le cas où le produit COTS ne répond pas aux

exigences de testabilité indiquées dans le SoW, il convient que l'ingénieur de développement mette en œuvre la partie manquante de la fonction de testabilité dans le système.

Le premier contractant pouvant ne pas être le vendeur des COTS, il est possible que les deux parties aient besoin de réaliser une évaluation en coopération. La quantité de test exigée assure que les articles COTS répondent aux exigences fonctionnelles et environnementales qui sont spécifiées pour le produit du premier contractant. Il peut s'avérer nécessaire d'exiger du fournisseur qu'il caractérise les données opérationnelles et environnementales et les résultats de test pour justifier les réclamations sur la fiabilité et la maintenabilité. Il peut également être nécessaire d'exiger que le fournisseur prouve que les procédés de fabrication ne compromettent pas les caractéristiques de fiabilité et de maintenabilité incluses dès la conception. Ces preuves peuvent comprendre les résultats des tests sur échantillons ou des tableaux de contrôle montrant que les procédés critiques sont maîtrisés avec une capacité du processus élevée.

6.4 Processus de développement de la testabilité

6.4.1 Support logistique

Il convient que le support de maintenance planifié du produit soit spécifié par le client dans le SoW afin que l'ingénieur de développement puisse déterminer les conséquences de l'attribution (par exemple priorité supérieure pour des fonctions TI). Si le produit à développer contient des unités matérielles normalisées remplaçables telles que des lampes, des fusibles, des filtres etc., il convient que le client détermine aussi l'attribution logistique de ces éléments dans le SoW (voir Figure 4 et Tableau 4).

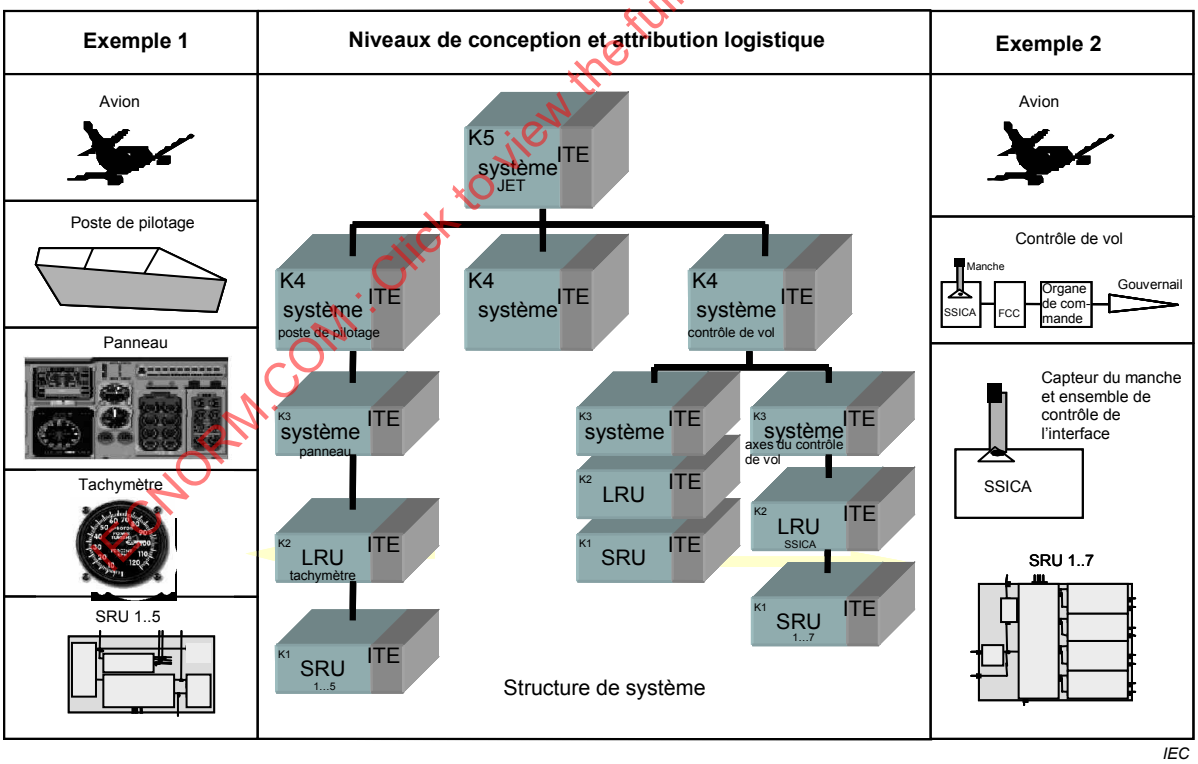


Figure 4 – Niveaux de conception et leur attribution logistique, prenant pour exemple un avion

Tableau 4 – Exemple d'attribution logistique

Niveau de conception	Attribution logistique	Exemple
K5		Avion
K4		Poste de pilotage, système de contrôle de vol
K3		Tableau 1, axe de contrôle de vol
K2	LRU	Tachymètre, SSICA
K1	SRU	Cartes enfichables, PCB

6.4.2 Testabilité et tests pour diagnostic

Dans la phase de conception et de développement, il convient que les principes et caractéristiques de testabilité soient intégrés dans la conception en accord avec les résultats des études initiales. Il convient de porter une attention particulière aux techniques de tests pour diagnostic qui peuvent améliorer la maintenabilité et minimiser les temps d'indisponibilité, et donc augmenter la disponibilité ainsi que les profits, tout en diminuant les coûts globaux.

Dans le cas de dispositifs ayant des caractéristiques inhérentes d'usure, ces améliorations concernent en premier lieu le coût de la maintenance préventive, qui peut être diminué de façon significative grâce à des procédures de tests pour diagnostic, particulièrement lorsque l'optimisation des intervalles de maintenance et de la quantité nécessaire de ressources et de maintenance préventive peut être réalisée. S'il n'y a pas de processus d'usure, comme c'est le cas pour la plupart des systèmes électroniques à semi-conducteurs, le coût de maintenance préventive est négligeable et l'impact des coûts les plus élevés est dû aux coûts d'investissement, qui sont eux-mêmes largement dépendants de la disponibilité obtenue. Dès lors que la majeure partie du temps d'indisponibilité est constituée par les temps de détection et de localisation de panne, les efforts consacrés aux diagnostics concernant ces éléments sont plus efficaces.

7 Attribution de testabilité

7.1 Généralités

Le but de cette partie du programme est de prouver, initialement par des moyens théoriques, plus tard par des moyens pratiques, que les exigences des tests pour diagnostic ont été satisfaites. Cela peut se réaliser à l'aide de méthodes et procédures similaires à celles appliquées pour la vérification des paramètres de maintenabilité (voir CEI 60706-3). Les concepts de vérification qu'il convient de prendre en considération comprennent

– la vérification par analyse;
– la vérification par tests.

7.2 Vérification par analyse

Les éléments de la vérification par analyse sont les suivants:

– revue de la documentation: il convient que les documents fournis en réponse aux exigences définies en 5 soient examinés eu égard à l'exhaustivité, la précision, la facilité d'utilisation;
– analyse: cette activité comprend les recherches analytiques sur le dispositif et l'évaluation de ses caractéristiques de testabilité en accord avec l'Annexe B.

7.3 Vérification par tests

Une vérification par tests est entreprise sur le matériel produit. Si cela est exigé dans le SoW, il convient donc de la réaliser au moment de l'acceptation des résultats de développement, et la spécification de test donne la base pour cette vérification. Une simulation de panne est effectuée au travers d'interventions non destructrices dans les unités matérielles et/ou, si nécessaire, une simulation par logiciel, mais il convient que celle-ci soit soutenue par des preuves pratiques. Pour les fonctions non testables, il faut que des preuves soient fournies pour justifier la conformité de la conception.

De plus amples informations sur la vérification de la testabilité sont données à l'Annexe B.

8 Documentation de testabilité

Le but de cette partie du programme est de s'assurer qu'une documentation complète du concept de diagnostic sera fournie sous une forme normalisée, de sorte que toute information pertinente soit rendue disponible pour les opérateurs et le personnel de maintenance du système. Il convient que la conception de la documentation tienne compte des conditions opérationnelles concernant à la fois l'utilisation et la maintenance, le concept de maintenance, les niveaux de compétence et le degré de la formation qui doit être dispensée. Plus de détails sur la documentation de la testabilité sont donnés dans l'Annexe B.

Annexe A
(informative)

Calculs des caractéristiques de reconnaissance de panne et de localisation de panne

A.1 Symboles

m nombre d'unités matérielles

n nombre de terminaux

h détection de panne en fonctionnement

k reconnaissance de panne en conditions de test

l localisation de panne au terminal

*v*1 localisation de panne sur 1 unité matérielle

*v*2 localisation de panne sur une des deux unités matérielles

*v*3 localisation de panne sur une des trois unités matérielles

A partie des tests pendant le fonctionnement (tests en ligne)

B partie des tests en conditions de test, sans équipement de test externe

C partie des tests en conditions de test, avec équipement de test externe (tests externes)

D partie de maintenance préventive (tests de maintenance)

A.2 Détection de panne en fonctionnement

Le symbole h_i signifie qu'une panne peut être détectée à un terminal *i* pendant le fonctionnement.

h_i = 1: détection de panne au terminal *i* en fonctionnement;

h_i = 0: pas de détection de panne au terminal *i* en fonctionnement;

$\sum_{i=1}^{n} h_i$ = nombre de terminaux où une panne peut être détectée pendant le fonctionnement.

Par conséquent, la caractéristique pour la reconnaissance de panne pendant le fonctionnement est la suivante:

$$FR_{(A)} = \frac{\sum_{i=1}^{n} h_i}{n} \times 100\ [\%]$$

A.3 Reconnaissance de panne en conditions de test

Le symbole k_i signifie qu'une panne peut être détectée à un terminal i dans des conditions de test.

k_i = 1: détection de panne à un terminal i dans des conditions de test;

k_i = 0: pas de détection de panne à un terminal i dans des conditions de test

$\sum_{i=1}^{n} k_i$ = nombre de terminaux où une panne peut être détectée en conditions de test.

Par conséquent, la caractéristique pour la reconnaissance de panne pendant le fonctionnement est la suivante:

$$FR_{(A+B+C+D)} = \frac{\sum_{i=1}^{n} k_i}{n} \times 100\ [\%]$$

A noter l'optimisation des chemins de test comme partie de la portion A de test (tests en ligne).

Dû à l'efficacité des coûts il peut être utile d'optimiser le nombre de chemins de test nécessaires pour la reconnaissance de panne pendant les tests en ligne au regard du taux de défaillance (λ) d'une sous-fonction.

FR = reconnaissance de panne (portion A) dépendant du taux de défaillance de la sous-fonction

SF = sous-fonction

P_{SFi} = nombre de ports testables de sous-fonction i

ΣP_{SFi} = somme de tous les ports de sous-fonction i

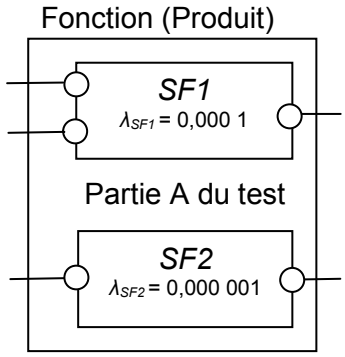
λ_{SFi} = taux de défaillance de la sous-fonction i

$\Sigma\lambda_{SFi}$ = somme de tous les taux de défaillance de sous-fonctions i

Formule:

$$FR = \sum_{i=1}^{n} \frac{P_{SFi}}{\sum P_{SFi}} * \frac{\lambda_{SFi}}{\sum \lambda_{SFi}} \leq 1$$

Exemple:



P_{SF1} = 3 λ_{SF1} = 0,0001

$\sum P_{SF1}$ = 3 λ_{SF2} = 0,000001

P_{SF2} = 2 $\sum \lambda_{SF}$ = 0,000101

$\sum P_{SF2}$ = 2

$$FR = (\frac{3}{3}) * (\frac{0{,}0001}{0{,}000101}) + (\frac{2}{2}) * (\frac{0{,}000001}{0{,}000101}) \leq 1$$

$$FR = (1) * (0{,}99) + (1) * (0{,}0099) \leq 1$$

$$FR = (0{,}99) * 100\% + (0{,}0099) * 100\% \leq 100\%$$

$$FR = (SF1)99\% + (SF2)1\% = 100\%$$

Résultat:

La probabilité que la sous-fonction *SF2* tombe en panne est de 1 %. Pour cette raison, les tests sur cette sous-fonction peuvent être transférés aux portions B ou C et donc minimiser l'effort de test pour les tests en ligne dans la portion A.

Localisation de panne

Le symbole l_i signifie qu'une panne peut être localisée au terminal *i*.

l_i = 1: localisation de panne au terminal *i*;

l_i = 0: pas de localisation de panne au terminal *i*;

$\sum_{i=1}^{n} l_i$ = nombre de terminaux où une panne peut être localisée.

Par conséquent, la caractéristique pour la localisation de panne au terminal est la suivante:

$$FL = \frac{\sum_{i=1}^{n} l_i}{n} \times 100\ [\%]$$

Le symbole $v1_j$ signifie qu'une panne peut être localisée de façon ambiguë sur une unité de matériel *j*.

$v1_j$ = 1: localisation de panne non ambiguë sur unité matérielle *j*;

$v1_j$ = 0: localisation de panne non ambiguë sur unité matérielle *j*;

$\sum_{j=1}^{m} v1_j$ = nombre d'unités matérielles lorsqu'une panne peut être localisée de façon non ambiguë.

Par conséquent, la caractéristique pour la localisation de panne sur une unité matérielle est la suivante:

$$FL_{v1} = \frac{\sum_{j=1}^{m} v1_j}{m} \times 100\ [\%]$$

Le symbole $v2_j$ signifie qu'une panne peut être localisée sur une des deux unités matérielles, dont l'une est l'unité *j*.

$v2_j$ = 1: localisation de panne sur l'unité matérielle *j* ou une autre unité matérielle;

$v2_j$ = 0: localisation de panne sur l'unité matérielle *j* ou une autre unité matérielle;

$\sum_{j=1}^{m} v2_j$ = nombre de cas où une panne peut être localisée sur une des deux unités matérielles.

Par conséquent, la caractéristique pour la localisation de panne sur une des deux unités matérielles est la suivante:

$$FL_{v2} = \frac{\sum_{j=1}^{m} v2_j}{m} \times 100\ [\%]$$

A.4 Exactitude du diagnostic et couverture de test

A.4.1 Symboles

En utilisant la notation de 5.4.3.1, les symboles suivants sont établis. Les valeurs A, B, C, D, sont les valeurs limites des sous-ensembles A', A'', B', B'' C', C'', D' et D''.

A	Tests pendant le fonctionnement (tests en ligne)	
A'	Tests en ligne menant à un diagnostic exact	(lim A' = A)
A''	Tests en ligne actuellement réalisés pour	(lim A'' = A)
B	Tests en conditions de test, sans équipement de test externe	(tests hors ligne)
B'	Tests hors ligne menant à un diagnostic exact	(lim B' = B)
B''	Tests hors ligne actuellement réalisés pour	(lim B'' = B)
C	Tests en conditions de test, avec équipement de test externe	(tests ext.)
C'	Tests externes menant à un diagnostic exact	(lim C' = C)
C''	Tests externes actuellement réalisés pour	(lim C'' = C)
D	Maintenance préventive (tests de maintenance)	
D'	Tests de maintenance menant à un diagnostic exact	(lim D' = D)
D''	Tests de maintenance actuellement réalisés pour	(lim D'' = D)

où A est la valeur limite de lim A'.

A.4.2 Exactitude de diagnostic

D'après les principes de base de la conception de testabilité, il convient que

A + B + C + D = 100 %

(voir 5.4.3.1), c'est-à-dire que toutes les pannes possibles sont diagnostiquées dans l'une ou l'autre des portions A, B, C D de la tâche de test. Le diagnostic est exact en sous-quantité

A' + B' + C' + D' ≤ 100 %

Par conséquent, l'exactitude D_c peut être exprimée par le rapport

$$D_c = \frac{A'+B'+C'+D'}{A+B+C+D} \leq 1$$

A.4.3 Couverture de test

Les pannes qui sont actuellement couvertes par une des portions A, B, C, D de la tâche de test sont contenues en sous-quantité

A'' + B'' + C'' + D'' ≤ 100 %

Par conséquent, la couverture de test T_c peut être exprimée par le rapport

$$T_c = \frac{A''+B''+C''+D''}{A+B+C+D} \leq 1$$

Annexe B
(informative)

Processus de développement pour produit testable

B.1 Analyse des exigences

B.1.1 Analyser les exigences de la définition du travail SoW

En utilisant les lignes directrices données dans cette norme, les exigences contenues dans le SoW sont analysées pour établir qu'elles sont complètes et sans ambiguïté.

Il convient de clarifier les exigences formulées qui ne sont pas claires en consultant le client et en les reformulant avec précision dans le SoW.

Une fois le SoW harmonisé et accepté par le client et le contractant, le contrat est conclu sur cette base.

B.1.2 Catégorisation du produit à développer

Les données de base du produit à développer (désignation, nombre d'entité, version, niveau de conception) sont déterminées sur la base du SoW accepté (voir Figure B.1).

Le niveau de conception à développer est dérivé des exigences du SoW (par exemple niveau de conception K4).

Les désignations logistiques (LRU/SRU) pour les unités matérielles remplaçables sont à adopter à partir du SoW.

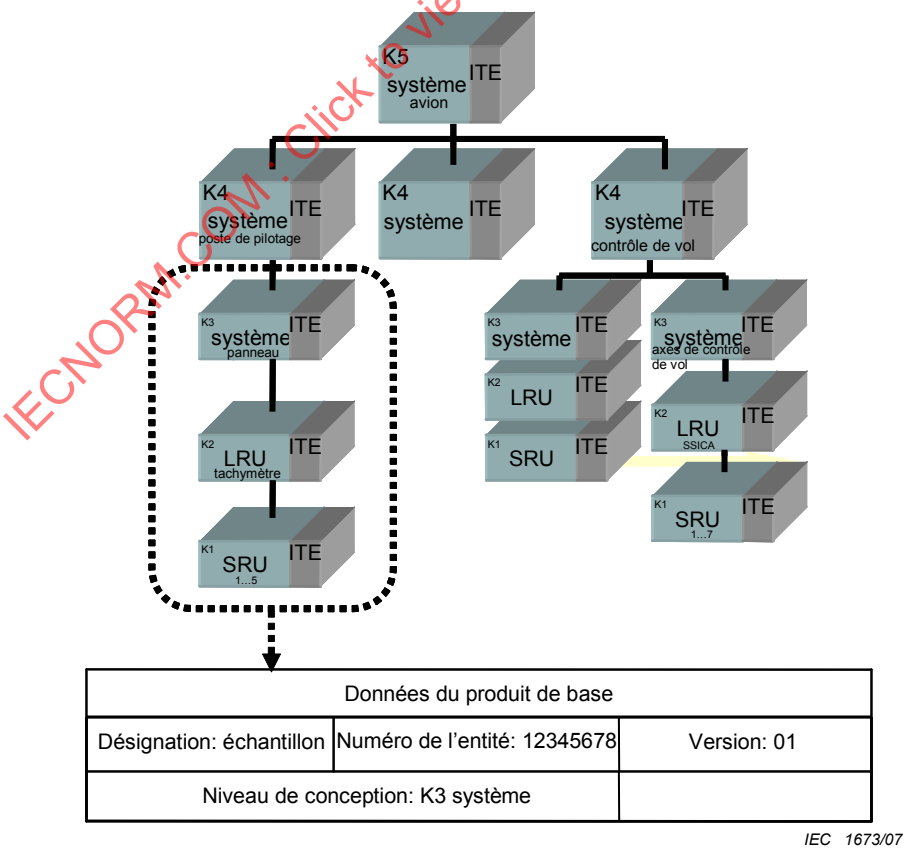


Figure B.1 – Exemple de méthode pour déterminer les données de base

Les données de base ont ainsi été déterminées.

B.2 Conception fonctionnelle

B.2.1 Lister les fonctions et sous-fonctions

Au début du développement, une structure fonctionnelle du produit en ligne avec la fonctionnalité nécessaire est effectuée sur la base de la définition du SoW accepté.

Une liste est établie des fonctions qui sont dérivées du SoW.

Ces fonctions sont déclinées en sous-fonctions indépendantes qui doivent être réalisées dans le niveau en question (voir Tableau B.1).

Règle: Etablir une liste de toutes les sous-fonctions SF qui sont à développer.

Tableau B.1 – Données pour le document «spécification du système»

Désignation: Echantillon Numéro d'entité: 12345678 Version: 01 **Niveau de conception: Système K3**	
Fonction	**Sous-fonction**
Fonction 1	SF1.1 SF1.2 SF1.3 SF1.4 SF1.5
Fonction 2	Non traité dans l'exemple
Fonction 3	Non traité dans l'exemple

B.2.2 Modélisation des fonctions et terminaux

Les données pour le document « spécification du système » sont utilisées pour la modélisation des sous-fonctions et terminaux du produit (voir Figure B.2).