BS EN 61069-5:2016

BSI Standards Publication

Industrial-process measurement, control and automation — Evaluation of system properties for the purpose of system assessment

Part 5: Assessment of system dependability

bsi.

National foreword

This British Standard is the UK implementation of EN 61069-5:2016. It is identical to IEC 61069-5:2016. It supersedes BS EN 61069-5:1995 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

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

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

Published by BSI Standards Limited 2016

ISBN 978 0 580 85995 3
ICS 25.040.40

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2016.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61069-5

September 2016

ICS 25.040.40

Supersedes EN 61069-5:1995

English Version

Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 5: Assessment of system dependability (IEC 61069-5:2016)

Mesure, commande et automation dans les processus industriels - Appréciation des propriétés d'un sytème en vue de son évaluation - Partie 5: Evaluation de la sûreté de fonctionnement d'un système (IEC 61069-5:2016)

Leittechnik für industrielle Prozesse - Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems - Teil 5: Eignungsbeurteilung der Systemzuverlässigkeit (IEC 61069-5:2016)

This European Standard was approved by CENELEC on 2016-07-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 61069-5:2016 E

European foreword

The text of document 65A/793/FDIS, future edition 2 of IEC 61069-5, prepared by SC 65A "System aspects", of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61069-5:2016.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2017-04-20
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2019-07-20

This document supersedes EN 61069-5:1995.

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

Endorsement notice

The text of the International Standard IEC 61069-5:2016 was approved by CENELEC as a European Standard without any modification.

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

IEC 60300-3-1:2003	NOTE	Harmonized as EN 60300-3-1:2004 (not modified).
IEC 60068	NOTE	Harmonized in EN 60068 series.
IEC 60812:2006	NOTE	Harmonized as EN 60812:2006 (not modified).
IEC 61000	NOTE	Harmonized in EN 61000 series.
IEC 61025:2006	NOTE	Harmonized as EN 61025:2007 (not modified).
IEC 61069-6	NOTE	Harmonized as EN 61069-6.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 61165	NOTE	Harmonized as EN 61165.
IEC 61326	NOTE	Harmonized in EN 61326 series.
IEC 61508	NOTE	Harmonized in EN 61508 series.

IEC 62443	NOTE	Harmonized in EN 62443 series [1)].
IEC/TS 62603-1	NOTE	Harmonized as CLC/TS 62603-1.

1) At draft stage.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60300-3-2	-	Dependability management - Part 3-2: Application guide - Collection of dependability data from the field	EN 60300-3-2	-
IEC 60319	-	Presentation and specification of reliability data for electronic components	-	-
IEC 61069-1	2016	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 1: Terminology and basic concepts	EN 61069-1	201X [2)]
IEC 61069-2	2016	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 2: Assessment methodology	EN 61069-2	201X [2)]
IEC 61070	-	Compliance test procedures for steady-state availability	-	-
IEC 61709	2011	Electric components - Reliability - Reference conditions for failure rates and stress models for conversion	EN 61709	2011
ISO/IEC 25010	-	Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models	-	-
ISO/IEC 27001	2013	Information technology - Security techniques - Information security management systems - Requirements	-	-
ISO/IEC 27002	-	Information technology - Security techniques - Code of practice for information security controls	-	-

2) To be published.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 5: Assessment of system dependability

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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 61069-5 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1994. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) reorganization of the material of IEC 61069-5:1994 to make the overall set of standards more organized and consistent;
b) IEC TS 62603-1 has been incorporated into this edition.

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

FDIS	Report on voting
65A/793/FDIS	65A/803/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 parts in the IEC 61069 series, published under the general title *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability 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.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

IEC 61069 deals with the method which should be used to assess system properties of a basic control system (BCS). IEC 61069 consists of the following parts.

Part 1: Terminology and basic concepts

Part 2: Assessment methodology

Part 3: Assessment of system functionality

Part 4: Assessment of system performance

Part 5: Assessment of system dependability

Part 6: Assessment of system operability

Part 7: Assessment of system safety

Part 8: Assessment of other system properties

Assessment of a system is the judgement, based on evidence, of the suitability of the system for a specific mission or class of missions.

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the specific mission or class of missions.

Since this is rarely practical, the rationale on which an assessment of a system should be based is:

– the identification of the importance of each of the relevant system properties,
– the planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various system properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of a system within practical cost and time constraints.

An assessment can only be carried out if a mission has been stated (or given), or if any mission can be hypothesized. In the absence of a mission, no assessment can be made; however, evaluations can still be specified and carried out for use in assessments performed by others. In such cases, IEC 61069 can be used as a guide for planning an evaluation and it provides methods for performing evaluations, since evaluations are an integral part of assessment.

In preparing the assessment, it can be discovered that the definition of the system is too narrow. For example, a facility with two or more revisions of the control systems sharing resources, for example a network, should consider issues of co-existence and inter-operability. In this case, the system to be investigated should not be limited to the “new” BCS; it should include both. That is, it should change the boundaries of the system to include enough of the other system to address these concerns.

The series structure and the relationship among the parts of IEC 61069 are shown in Figure 1.

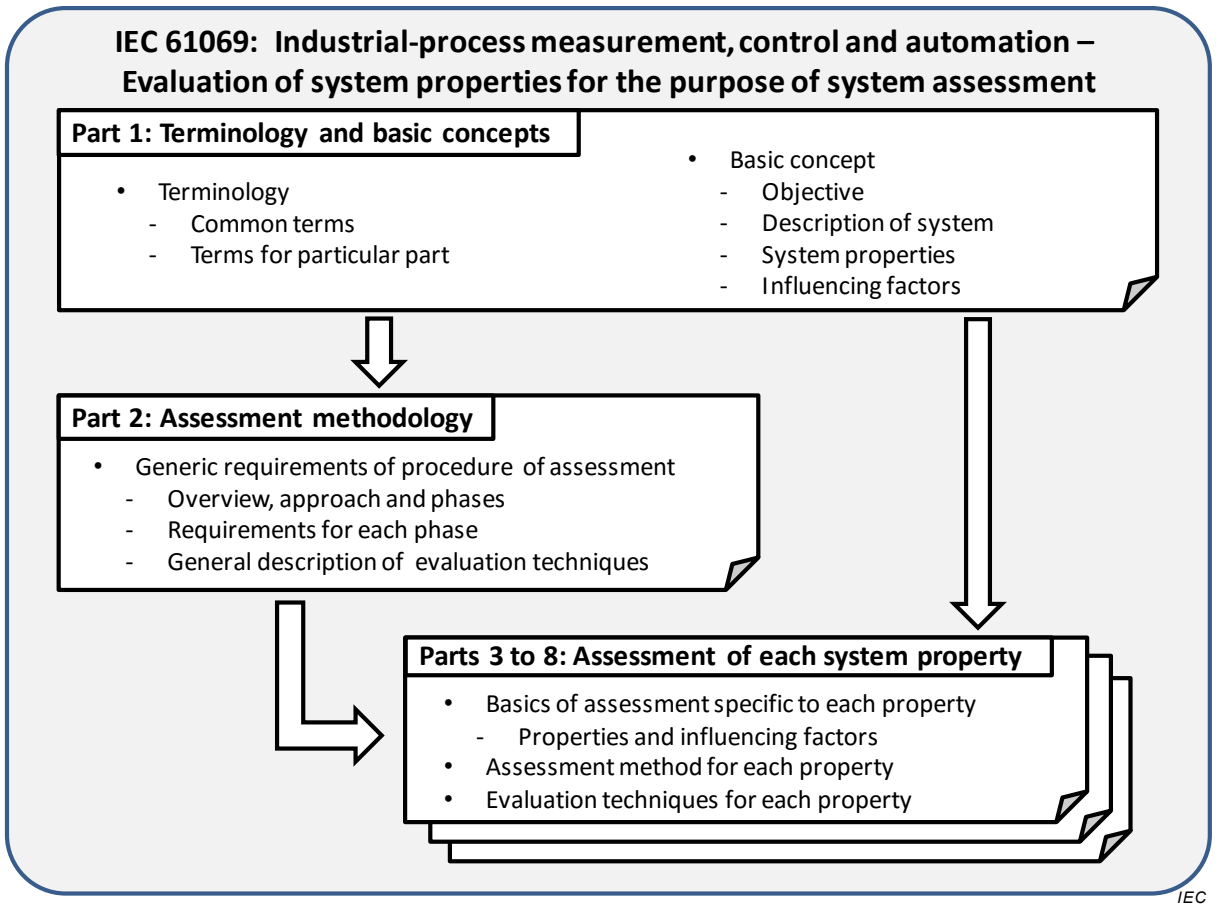

Figure 1 – General layout of IEC 61069

Some example assessment items are integrated in Annex C.

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 5: Assessment of system dependability

1 Scope

This part of IEC 61069:

– specifies the detailed method of the assessment of dependability of a basic control system (BCS) based on the basic concepts of IEC 61069-1 and methodology of IEC 61069-2,

– defines basic categorization of dependability properties,

– describes the factors that influence dependability and which need to be taken into account when evaluating dependability, and

– provides guidance in selecting techniques from a set of options (with references) for evaluating the dependability.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC 60319, *Presentation and specification of reliability data for electronic components*

IEC 61069-1:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 1: Terminology and basic concepts*

IEC 61069-2:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

IEC 61070, *Compliance test procedures tor steady-state availability*

IEC 61709:2011, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

ISO IEC 25010, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*

ISO IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

ISO IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61069-1 apply.

3.2 Abbreviated terms, acronyms, conventions and symbols

For the purposes of this document, the abbreviated terms, acronyms, conventions and symbols given in IEC 61069-1 apply.

4 Basis of assessment specific to dependability

4.1 Dependability properties

4.1.1 General

To fully assess the dependability, the system properties are categorised in a hierarchical way.

For a system to be dependable it is necessary that it is ready to perform its functions. However, in practice, when the system is ready to perform its function, this does not mean that it is sure that the functions are performed correctly. In order to cover these two aspects, dependability properties are categorised into the groups and subgroups shown in Figure 2.

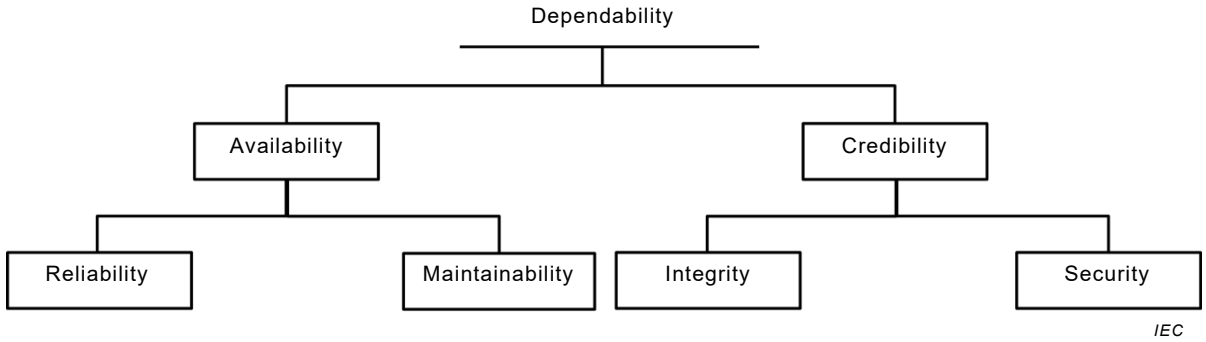

Figure 2 – Dependability

Dependability cannot be assessed directly and cannot be described by a single property. Dependability can only be determined by analysis and testing of each of its properties individually.

The relationship between the dependability properties of the system and its modules is sometimes very complex.

For example:

– if the system configuration includes redundancy, availability property of the system is dependent upon the integrity properties of the redundant modules;
– if the system configuration includes system security mechanisms, security property of the system is dependent upon the availability properties of modules that perform the security mechanism;
– if the system configuration includes modules that check data transferred internally from other parts of the system, then integrity property of the system is dependent upon the security properties of these modules.

When a system performs several tasks of the system, its dependability can vary across those tasks. For each of these tasks, a separate analysis is required.

4.1.2 Availability

Availability of the system is dependent upon the availabilities of the individual modules of the system and the way in which these modules cooperate in performing tasks of the system. The way in which modules of the system cooperate can include functional redundancy (homogeneous or diverse), functional fall-back and degradation. Availability is dependent in practice upon the procedures used and the resources available for maintaining the system. The availability of the system can differ with respect to each of its tasks.

Availability of the system for each task can be quantified in two ways:

A system's availability can be predicted as:

Availability = mean_time_to_failure / (mean_time_to_failure + mean_time_to_restoration)

where:

- "availability" is the availability of the system for the given task;
- "mean_time_to_failure" is the mean of the time from restoration of a system into a state of performing its given task(s) to the time the system fails to do so;
- "mean-time_to_restoration" is the mean of the total time required to restore performance of the given task from the time the system failed to perform that task.

For a system in operation, the availability can be calculated as:

Availability = total_time_the_system_has_been_able_to_perform_the_task / Total_time_the_system_has_been_expected_to_perform_the_task

4.1.3 Reliability

Reliability of a system is dependent upon the reliability of the individual modules of the system and the way in which these modules cooperate in performing task(s) of the system. The way in which these modules cooperate can include functional redundancy (homogeneous or diverse), functional fall-back and degradation.

Reliability of the system can differ with respect to each of its tasks. Reliability can be quantified for individual tasks, with varying degrees of predictive confidence.

The reliability of the individual elements of the system can be predicted using the parts count method (see IEC 62380 and IEC 61069-6). Reliability of the system can then be predicted by synthesis. It should be noted, that for the software modules of systems, there are no reliability prediction methods available that provide high levels of confidence.

Mechanisms to analyse software reliability are described in ISO IEC 25010.

Reliability can be represented by mean time to failure (MTTF) or failure rate.

4.1.4 Maintainability

The maintainability of a system is dependent upon the maintainability of individual elements and structure of elements and modules of the system. The physical structure affects ease of access, replaceability, etc. The functional structure affects ease of diagnosis, etc.

When quantifying the maintainability of a system, all actions required to restore the system to the state where it is fully capable of performing its tasks should be included. This should include actions such as the time necessary to detect the fault, to notify maintenance, to diagnose and remedy the cause, to adjust and check, etc.

The quantification of maintainability should be augmented with qualitative statements by checking the provision for and the coverage of the following items:

The quantification of maintainability should be augmented with qualitative statements by checking the provision for and the coverage of the following items:

– notification of the occurrence of the failures: lights, alert messages, reports, etc.;
– access: ease of access for personnel and for connecting measuring instruments, modularity, etc.;
– diagnostics: direct fault identification, diagnostic tools which have no influence on the system by itself, remote maintenance support facilities, statistical error checking and reporting;
– repairability/replaceability: few restrictions on the replacement of modules while operating (“hot swap” support), modularity, unambiguous identification of modules and elements, minimum need for special tools, minimum repercussions on other elements or modules, when elements or modules are replaced;
– check-out: guided maintenance procedures, minimum check-out requirements.

Maintainability can be represented by mean time to repair (MTTR).

4.1.5 Credibility

The credibility of a system is dependent upon the integrity and security mechanisms implemented as functions performed by the modules of the system.

Credibility mechanisms include:

– a check on
  - correct performance of functions (for example by watchdog, using known data); and/or
  - correct data (for example validity check, parity check, readback, input validation, etc.);
– an action, such as:
  - self-correction;
  - confinement;
  - notification of action, etc.

These mechanisms can be used to provide integrity and/or security.

To analyse the credibility mechanisms, the fault injection techniques described in 6.1 can be used.

Credibility is deterministic and some aspects can be quantified.

4.1.6 Security

The security of a system is dependent upon mechanisms implemented at the boundary of the system to detect and prevent incorrect inputs and unauthorized access. These boundaries can be physical or virtual. See:

– Annex F for more considerations on security, and
– IEC 62443 series.

A security mechanism can be implemented by an element checking the inputs to other elements.

4.1.7 Integrity

The integrity is dependent upon mechanisms implemented at the output elements of the system to check for correct outputs. It also depends upon mechanisms implemented within the system to detect and prevent incorrect transitions of signals or data between parts of the system.

An integrity mechanism is implemented by an element checking the outputs of other elements.

4.2 Factors influencing dependability

The dependability of a system can be affected by the following influencing factors listed in IEC 61069-1:2016, 5.3.

For each of the system properties listed in 4.1, the primary influencing factors are as follows:

– Reliability is influenced by the influencing factors;
  - utilities, the influence is partly predictable using IEC 61709,
  - environment, the influence is partly predictable using IEC 61709,
  - services, due to the handling, storage of parts, etc.
– Maintainability; for the purpose of this standard, maintainability is considered as an intrinsic property of the system itself and is only affected in an indirect way, for example restricted access due to hazardous conditions.
– Availability; when taking into account the human activities necessary to retain the system in, or restore the system to, a state in which the system is capable of performing task(s) of the system, availability is influenced by human behaviour and service conditions (delays in delivery of spare parts, training, documentation, etc.).
– Credibility; the mechanisms (security and integrity) can be affected by intentional or unintentional human actions and by infestations of pests and if these mechanisms share common facilities, such as buses or multitasking processors, they can be influenced by task(s) of the system, the process due to a sudden increase in process activity (for example an alarm burst), etc. and external systems.

In general, any deviations from the reference conditions in which the system is supposed to operate can affect the correct working of the system.

When specifying tests to evaluate the effects of influencing factors, the following standards should be consulted:

– IEC 60068,
– IEC 60801,
– IEC 61000, and
– IEC 61326.

5 Assessment method

5.1 General

The assessment shall follow the method as laid down in IEC 61069-2:2016, Clause 5.

5.2 Defining the objective of the assessment

Defining the objective of the assessment shall follow the method as laid down in IEC 61069-2:2016, 5.2.

5.3 Design and layout of the assessment

Design and layout of the assessment shall follow the method as laid down in IEC 61069-2:2016, 5.3.

Defining the scope of assessment shall follow the method laid down in IEC 61069-2:2016, 5.3.1.

Collation of documented information shall be conducted in accordance with IEC 61069-2:2016, 5.3.3.

The statements compiled in accordance with IEC 61069-2:2016, 5.3.3 should include the following in addition to the items listed in IEC 61069-2:2016, 5.3.3.

– No additional items are noted

Documenting collated information shall follow the method in IEC 61069-2:2016, 5.3.4.

Selecting assessment items shall follow IEC 61069-2:2016, 5.3.5.

Assessment specification should be developed in accordance with IEC 61069-2:2016, 5.3.6.

Comparison of the SRD and the SSD shall follow IEC 61069-2:2016, 5.3.

NOTE 1 A checklist of SRD for system dependability is provided in Annex A.

NOTE 2 A checklist of SSD for system dependability is provided in Annex B.

5.4 Planning of the assessment program

Planning the assessment program shall follow the method as laid down in IEC 61069-2:2016, 5.4.

Assessment activities shall be developed in accordance with IEC 61069-2:2016, 5.4.2.

The final assessment program should specify points specified in IEC 61069-2:2016, 5.4.3.

5.5 Execution of the assessment

The execution of the assessment shall be in accordance with IEC 61069-2:2016, 5.5.

5.6 Reporting of the assessment

The reporting of the assessment shall be in accordance with IEC 61069-2:2016, 5.6.

The report shall include information specified in IEC 61069-2:2016, 5.6. Additionally, the assessment report should address the following points:

– No additional items are noted.

6 Evaluation techniques

6.1 General

Within this standard, several evaluation techniques are suggested. Other methods may be applied but, in all cases, the assessment report should provide references to documents describing the techniques used.

Those evaluation techniques are categorized as described in IEC 61069-2:2016, Clause 6.

Factors influencing dependability properties of the system as per 4.2 shall be taken into account.

The techniques given in 6.2, 6.3 and 6.4 are recommended to assess dependability properties.

Quantitative evaluation can be based on a predictive analysis, calculations, or on tests.

To start the evaluation it is first necessary to analyse the functional and physical structure of the system. Once this is accomplished an analysis of how the tasks are performed by the system should be done.

The structure of the system can be described using functional and physical block diagrams, signal flow diagrams, state graphs, tables, etc.

Failure modes are considered for all elements (hardware and software). Their effects on the dependability of the task(s) of the system, together with the influence of the requirements for maintainability, are determined.

Quantitative evaluations can be performed using one of, or a combination of, the available methods described in 6.2 and 6.3.

The analysis shall include an examination of the manner in which alternative paths through the system are initiated, i.e.:

– in a static manner by changing the system configuration; or
– dynamically, either automatically, for example, by credibility mechanisms or manually, for example, by a keyboard action.

A list of items that shall be considered for the assessment can be found in IEC 60319 and IEC 61709. The analytical techniques, described below, are based on models. Such models can rarely represent the real system exactly, and, even if they can, there can never be 100 % certainty that they do. The evaluation results based on analytical techniques should therefore also state their confidence level.

The dependability of a system is also influenced by errors introduced into the system during the design, specification and manufacturing stages. This holds equally well for the hardware and software of the system. These errors can only be discovered by meticulously checking the proper execution of each function.

In addition, injecting hypothetical faults or errors is a valuable technique in providing an increase in the degree of confidence in the final dependability of the system, as achieved during all stages of the design, specification and manufacturing. These fault injection techniques can be accomplished by using hardware and/or specially designed software. They are used to discover what the overall consequence, to the task(s) of the system, will be.

It should however be recognized that, in practice, the increase in confidence is limited since the number of tests that can be designed and carried out will be constrained by the number of all possible errors and faults that can be thought of and injected.

NOTE An example of a list of assessment items is provided in Annex C.

6.2 Analytical evaluation techniques

6.2.1 Overview

This subclause discusses common analytical evaluation techniques: logical analysis (inductive and deductive) and predictive evaluation.

6.2.2 Inductive analysis

At the component or element level the failure modes are identified and for each of these modes the corresponding effect on the dependability of the system task(s) at the next higher level is analysed. The resulting failure effects become the failure modes at the next higher level.

This "bottom-up" approach is a tedious method which finally results in the identification of the effects at all levels of the system of all postulated failure modes.

An appropriate inductive analysis method is described in IEC 60812.

6.2.3 Deductive analysis

Deductive analysis proceeds from a hypothetical failure at the highest level in the system, i.e. the failure of a task, to successively lower levels.

The next tower level is analysed to identify failure modes and associated failures, which would result in the identified failure at the highest level, i.e. the task level.

The analysis is repeated by tracking back through the functional and physical paths of the system until the analysis yields sufficient information in terms of dependability (including maintainability) for the assessment.

The deductive analysis does not give any information on failure modes that are not postulated as events. It is however very time effective for complex systems, for which it is more convenient to describe what is considered a system failure or success, than to consider all the possible failure modes of the constituent elements of the system.

An appropriate deductive analysis method is described in IEC 61025.

6.2.4 Predictive evaluation

A predictive evaluation is based on a qualitative analysis complemented with quantification of the basic reliability (failure rates) of the elements. To quantify the failure rate of the system to perform its task(s), a predictive analysis method is required. An appropriate method is described in IEC 61078.

A reliability block diagram can be constructed almost directly from the functional and physical structure of the system. The method is primarily oriented towards success analysis (two-state) and does not deal effectively with complex repair and maintenance strategies nor with multi-state situations.

Various mathematical tools are available in support of the calculation of the failure rates such as boolean algebra, truth tables and/or path and cut set analysis. To predict quantitatively failure rates of a system to perform its task in a multi-state situation, an analysis method such as described in IEC 61165 may be used.

The Markov analysis method, however, becomes very complex if a large number of system states are to be considered. In such cases it is more effective to apply the Markov analysis to calculate reliability data for subsets of analysis models derived with one of the other analysis methods, such as "fault tree analysis".

Basic quantified failure rate data for the modules and elements used in the above analysis methods can be obtained from field experience or via a calculation method "parts count reliability prediction" using generic data for the components of the modules and elements. The parts count reliability prediction method is described in IEC 61709.

To account for stress levels due to influencing factors, the method described in IEC 61709 and the information listed in Annex A should be used.

The parts count method is based on the assumption that the components are functionally connected in series (worst case estimate). The components of the modules of the system and elements are listed per module or element, stating for each component its type, its appropriate failure rate, the factors influencing the failure rate (part quality, environment, etc.) and the number used.

Alternatively generic failure data may be found in the references contained in Annex E.

For complex systems, such as BCSs, it is impossible in practice to make an accurate predictive assessment of the dependability properties.

The system properties, maintainability, security, and integrity, depend mainly on the features designed into the system, and hence the degree of their existence cannot be calculated in a probabilistic manner. The reliability of the elements used to assure security and integrity shall be considered. The methods used to assess the reliability of these elements may be the same as those used for the elements and modules supporting the primary system functions.

6.3 Empirical evaluation techniques

6.3.1 Overview

To rely solely upon system-level testing to measure reliability and availability for a complex system is neither practical nor cost-effective. In general, complex systems are unique (number of samples equals one). Furthermore, the coverage of such tests will of necessity be severely constrained by the time allowed for the tests. However, for systems which are already in operation such tests provide valuable information.

The actual data obtained in this way is useful for:

– guiding improvement of future designs, structure of system, redesign or replacement of failure prone equipment and software;
– comparison of expected or specified characteristics with actual data;
– generating field data that can be used for future dependability predictions.

Guidance on procedures that shall be followed for defining test can be found in IEC 61070 and IEC 60300-3-2.

The main objective of performing tests on systems is to evaluate the behaviour of a system on the occurrence of a fault (hardware and software) or of an unauthorized or incorrect input (integrity and security).

To observe the behaviour of a system, a representative task or set of tasks shall be defined and for each task those system states that are considered to be a failure shall be defined (for example state of the output(s)). Guidance on the treatment of these tests can be found in IEC 60706-4.

6.3.2 Tests by fault-injection techniques

Prior to testing by fault injection, the system specification should be examined to determine:

– the integrity measures taken to avert the propagation of faults through the system;
– the security measures taken to avert the intrusion of faulty or unauthorized inputs; the diagnostic features provided.

To be time-effective, the design of system tests should be based on a qualitative analysis and, as far as possible, should use the diagnostic features provided by and for the system. Care should be taken that, where these diagnostic features are necessary to provide the system dependability, these themselves should be tested independently.

To test integrity, faults can be injected into module(s), element(s) and/or component(s). Observations are then made to determine if:

– the system outputs fail; and/or
– notice is given of the fault.

To test security, faults can be injected or unauthorized information entered at the system boundaries, i.e. incorrect inputs, human error in operation and/or maintenance activities.

Care should be taken to include some simultaneous tests of both integrity and security. The result of some faults can be the lack of detection of the fault, i.e. an undetectable fault. Therefore care should be taken to include some simultaneous tests of both integrity and security. Annex D lists a number of faults which may be introduced when executing these tests.

6.3.3 Tests by environmental perturbations

Some perturbations of the influencing factors can trigger the security mechanisms.

Therefore, selected influencing factors should be varied around their normal values to test the security mechanisms.

For the selection of the influencing factors refer to 4.2.

6.4 Additional topics for evaluation techniques

No additional items are noted.

Annex A
(informative)

Checklist and/or example of SRD for system dependability

The system requirements document should be reviewed to check that for each of the system tasks the following are clearly stated:

– the relative importance of the task;
– the definition of what is considered to be a failure of the task;
– the criteria of the failure in terms of the dependability properties;
– the operational and operating environment.

The specification of a failure in quantitative or qualitative terms should follow a format defined before the evaluation and assessment begins.

Annex B
(informative)

Checklist and/or example of SSD for system dependability

B.1 SSD information

The system specification document should be reviewed to check that the properties given in the SRD are listed as described in IEC 61069-2:2016, Annex B.

B.2 Check points for system dependability

Particular attention should be paid to verify that information is given on:

– the system functions supporting each task and the modules and elements, both hardware and software, supporting each of these functions;
– the alternative routes supported by the system to perform each task and how these alternative routes are activated;
– credibility mechanisms (security and integrity) provided and how these are supported;
– reliability and availability of each task as well as of the supporting functions, modules and elements;
– maintainability characteristics;
– operational and environmental characteristics and limits of use for the modules and elements.

Annex C
(informative)

An example of a list of assessment items (information from IEC TS 62603-1)

C.1 Overview

Annex C provides some examples about influencing factors related to this standard which were extracted from IEC TS 62603-1.

The classifications of values of properties described in this standard are only examples.

C.2 Dependability

Dependability cannot be described by a single number. Some of its properties can be expressed as probabilities, other properties are deterministic; some aspects can be quantified, other aspects can only be described in a qualitative way.

When a system performs several tasks of the system, its dependability may vary across those tasks. For each of these tasks, a separate analysis is required.

C.3 Availability

C.3.1 System self-diagnostics

System self-diagnostics allow one to rapidly recognize the failure and thus reduce the mean time to repair. For that reason, assessors should consider the systems self-diagnostic capabilities at all levels of the system.

It could be necessary to implement self-diagnostic routines for the basic components of the BCS, such as the I/O cards or modules, the processor card, the memory cards and the communication links.

The self-diagnostic of field devices should be implemented in the control logic to actuate safety or recovery actions in case of field errors. Self-diagnostic of other components of the BCS are a part of the alarm management system.

C.3.2 Single component fault tolerance and redundancy

C.3.2.1 Overview

Fault tolerance is the built-in capability of a system to provide the continued, correct execution of its assigned function(s) in presence of a hardware or software failure of a single component. In other words, the system is able to perform its mission even after the first failure (hardware or software).

C.3.2.2 Redundancy criteria

When specifying a control system, the effects of component failure should be assessed in relation to the controlled process, and redundancy should be requested accordingly.

Redundancy should cover components that are critical or vital for proper and safe operation of the entire system. When defining redundancy criteria, the following requirements should be addressed, when applicable according to the type of component:

– the type of stand-by, if any,
– the management of the software and data back-up between the redundant components;
– redundancy policy (1-out-of-2, 2-out-of-3, k-out-of-m);
– synchronization of data between the active and the stand-by machines;
– configuration of the active and stand-by machine.

It is particularly useful to examine the availability of fault-tolerance and/or redundancy in:

– power supplies including UPS backup;
– I/O modules;
– I/O networks between I/O modules and controllers;
– controllers;
– control networks linking controls, workstations and other components;
– operator workstations, for example, can replace any workstation;
– servers.

Characteristics of importance include:

– bumpless failover;
– failover time (time when a service is not available);
– failure modes (can some modes of failure cause both the primary and secondary to be lost).

C.3.3 Redundancy methods

C.3.3.1 General

Availability of the system depends upon the availabilities of the individual parts of the system and the way in which these parts cooperate in performing the tasks of the system. The way in which parts cooperate may include:

– functional redundancy (homogeneous or diverse): the redundancy of a specific function can be obtained using the same hardware both for the master and the stand-by (homogeneous) or with independent hardware (diverse). If functional redundancy is available, the first failure does not reduce the functionalities and the performances of the system;
– functional fall-back: is the capacity of returning to a known functional level or mode in case of failure or abnormal operation;
– degradation: in case of failure of a part of the BCS, the performances and the functionalities of the system are reduced. In degraded working condition all the critical functions are properly working.

Availability depends upon the procedures used and the resources available for maintaining the system. Availability requirements are usually expressed as the accumulated down times occurring over a certain period of time. Different availability values are possible for different tasks of the BCS.

In addition to the desired downtime, further special needs, if any, for increasing the availability of some critical functions should be specified in terms of component redundancy.

C.3.3.2 Admissible degraded conditions

Because of faults in the system, the entire system cannot achieve all the functions that represent its mission. If degraded working conditions are admissible, it is possible to keep the process and the system running even if one or more functions abort. It is necessary to identify which are the functions that are not critical for the operation of the system and that can be lost in degraded conditions. The capacity of operating in degraded conditions increases the availability of the BCS.

C.3.3.3 Stand-by configurations

If some critical components are redundant, it is necessary to define the stand-by configuration. Basically, there are two possible stand-by configurations:

– hot stand-by: the primary and the back-up components or systems run simultaneously. Data, if the component should process data, are mirrored to the back-up component in real-time so that the two components are identical. The system can perform a hot swap between the primary and the back-up component without losing any data;

– cold stand-by: in this configuration the back-up component is called up only when the primary component fails. Data, if needed, are mirrored in the back-up component with an update rate lower than in the case of the hot stand-by. This configuration is used for non-critical applications.

Intermediate solutions between hot and cold stand-by may exist, and are sometime referred as “warm stand-by”.

C.3.3.4 Protection action in fail-safe mode

The concept of fail-safe is a protection against the effect of failure of equipment. The fail-safe mode refers to the capacity to switch into a predetermined safe state when a specific malfunction occurs. For performing a fail-safe protection, it is necessary to define the fail-safe devices (i.e. components, systems, control devices, etc.) that are designed so that they set the controlled parameters in a predetermined (safe) condition when a failure is detected.

It should be defined the actions that a fail-safe device implements when it is requested to act as fail-safe device. For example, for a fail-safe valve, the protection action can be the open or the close position.

C.3.3.5 Hot swappable components

Each component of the BCS is hot swappable if it can be removed and substituted while the BCS is operating. The BCS automatically configures the new component as previously configured the removed one. Hot-swap is possible both with faulted components, and with sound ones. The hot swap capability is often required for critical components, whose failure might jeopardize one or more functions of the BCS. For this reason, hot swappable components usually have an installed back-up. The BCS technical specification should indicate the critical components that need a hot swap (if any).

C.4 Reliability

Reliability of a system depends upon the reliability of the individual parts of the system and the way in which these parts cooperate in performing the system task(s). The way in which parts cooperate may include functional redundancy (homogeneous or diverse), functional fallback and degradation. Reliability of the system may differ with respect to each of its tasks. Reliability can be quantified for individual tasks, with varying degrees of predictive confidence. The reliability of the individual hardware parts of the system can be predicted using the parts count method (see IEC 62380). Reliability of the overall system can be calculated by analytical tools and methods (see IEC 61078 and IEC 61025). It should be noted that for the software modules of systems, there are no reliability prediction methods available that provide high levels of confidence.

C.5 Maintainability

C.5.1 General

Maintainability is the ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.

C.5.2 Generation of maintenance requests

The system can generate maintenance requests if the operating status of a component changes. The capacity of generating a maintenance request is a way towards the preventive-predictive maintenance; devices or sub-systems recognize autonomously the need for a repair intervention before failures arise. This capacity is mainly related to intelligent field devices such as analytical instruments, valve positioners, etc.

C.5.3 Strategies for maintenance

Different strategies for maintenance exist, as reported in the following:

– corrective maintenance: response to existing fault and diagnostic messages. Maintenance means here to repair or replace the faulted element;

– preventive maintenance: appropriate maintenance measures are initiated before a failure occurs. Maintenance means here to perform a time-dependant or status-dependant repair or replace policy;

– predictive maintenance: predictive diagnostics for timely detection of potential problems and to determine the remaining service life. Maintenance means here to schedule appropriate repair or substitution interventions based on measured data.

In the definition of the requirements, the requested strategies for maintenance should be defined.

C.5.4 System software maintenance

According to ISO IEC 14764, the software maintenance is the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.

The BCS software maintenance includes the installation of patches, upgrades or new releases of firmware.

The user should require a service of software upgrade from the contractor. This service includes any new release (major or minor, depending on the contract) or patch that is developed by the contractor during the service period.

The software upgrade service can be limited to the sole delivery of the new releases and patches, or can also include the installation of the upgraded software on the system itself.

The contractor should notify the user about the compatibility of all major official operating system patches or security updates with the system. If required, the user should include in the software upgrade service also the installation of the official operating system patches and security updates.

C.6 Credibility

Credibility depends:

– on the ability of the system to provide warning should it fail into a state in which it is not able to perform some or all of its functions correctly (integrity);
– on the ability of the system to reject any incorrect inputs or unauthorized access to the system (security).

C.7 Security

See Annex F.

C.8 Integrity

C.8.1 General

The following C.8.2 to C.8.10 discuss some of the items to investigate with regard to integrity of the data processed by the system.

C.8.2 Hot-swap

Hot-swap for I/O cards or modules should be specified separately, considering the higher stress and rate of failure of these devices.

C.8.3 Module diagnostic

The BCS monitors the operating status of each I/O card or module. Both normal and abnormal operation, e.g. faults or withdrawal, are displayed on the HMI.

C.8.4 Input validation

When a SPDT contact is acquired as two digital inputs, validation logic is implemented to detect abnormal statuses. Similarly, the out-of-range of an analogue signal is detected when the signal rises above or drops below the valid range.

C.8.5 Read-back function

Analogue and digital outputs of the BCS are sent back to input cards to implement validation logic. For example, this function may be used to verify the emission of open/close commands or the value of emitted set-points.

C.8.6 Forced output

Each digital and/or analogue output is forced to a pre-defined value, singularly settable, in case of faults or abnormal operation.

C.8.7 Monitoring functions

The input cards are designed to detect the most common failures in field, i.e. open or broken circuit.

C.8.8 Controllers

Things to assess include:

– use of error correcting RAM;
– approach to fault-tolerance / redundancy and the resulting data consistency issues, e.g., assurance that no “bad” data can be sent to the field in the event of failure of the primary controller.

C.8.9 Networks

Things to assess include:

– integrity checks on the messages, e.g., error correcting codes;
– timeouts on communications;
– status bits associated “atomically” with value so that application can judge data quality.

C.8.10 Workstations and servers

Things to assess include:

– error correcting RAM.

Annex D
(informative)

Credibility tests

D.1 Overview

The testing by injecting faults into the system provides a useful contribution to assessing the credibility of systems (hardware and software).

These techniques require an in-depth knowledge by the test personnel of the system operation and its physical and functional structure and make it often necessary to access the system physically.

The philosophy behind these tests is the following: a credible system should not fail to perform tasks correctly, despite a failure of an element or an attempt on the system through its boundary.

To test this, faults are created (to test integrity) and/or alternatively a non-authorized or wrong operation is introduced (to test security) and the resulting system behaviour (state of the output(s) and/or signalling reporting provided) is observed.

Below are examples of questions that need to be addressed regarding system behaviour:

– are the outputs driven to or frozen into a predefined position when a fault occurs?
– is the keyboard automatically blocked when a screen is not operating correctly?
– how does the system behave when communication is overloaded?
– is signalization provided by the watchdog, alarm, printing facilities, when a fault is injected?

On the basis of a qualitative analysis, a coordinated approach to the tests should be adopted, starting at board level and moving gradually to the integrated circuit pin level to avoid unnecessary work.

In general, single steady faults are introduced. The types of faults injected are, for example:

– board or module removal;
– opening of board connections (most system failures are due to bad connections);
– opening of IC's pins or forcing them to represent a "logic" 0 or 1.

Special arrangements may be required to be able to perform the tests, such as:

– extender boards with switches;
– clamps;
– special test software.

Depending on the depth of the assessment, the method may be time-consuming, but has the advantage that it is easy to implement and that the test facilities required are relatively inexpensive.

NOTE Care and precaution are taken when implementing these tests in order to avoid damage of some of the elements in the system.

D.2 Injected faults

D.2.1 General

Potential failure modes of the systems are classified in 5.2.3 of IEC 60812:2006.

A number of faults are identified in the following subclauses which may lead to a system failure and can be used for simulation.

D.2.2 System failures due to a faulty module, element or component

System failures may result from faults caused by support capabilities, high temperatures, functional capabilities, such as:

– loss of power of single power supply units;
– loss of power of redundant power supply units (active as well as passive unit);
– loss of power to redundant modules, primary as well as secondary side of the power supply module;
– loss of power to single modules and elements;
– loss of communication buses between modules and elements, single and redundant;
– loss of a module or element;
– loss of power to peripheral equipment (screens, keyboards, printers, disk drives, etc.);
– loss of communication to peripheral equipment;
– open- and short-circuits of power lines, communication buses, address lines, input/output lines.

D.2.3 System failures due to human errors

System failures may result from faults caused by incorrect maintenance operations, reconfiguration, software updates, such as:

– mixing-up redundant bus cables;
– setting incorrect address of modules, elements, etc.;
– inserting printed circuit boards in wrong positions;
– inserting printed circuit boards in upside-down positions;
– inserting connectors in upside-down or reverse positions;
– inserting connectors in wrong positions;
– failing to insert connectors after repair;
– reversing the power connections;
– failing to execute a complete or correct initialization or start-up procedure;
– using the same address twice. etc.

D.2.4 System failures resulting from incorrect or unauthorized inputs into the system through the man-machine interface

System failures may result from faults caused by poor training, ergonomics, confusing user interface such as:

– call-up or use of non-existing or incorrect displays, tag-codes, programs or peripherals;
– creating overflow conditions at keyboard or touch screen by introducing a large number of commands in a short time (n-key roll over);
– use of incomplete codes at call-up of displays, tags, etc.

D.3 Observations

When the above faults are injected, the following questions are asked and the responses recorded.

– Which tasks of the system are affected and how are they affected?
  - Will changes of input signals still be detected in all corresponding modules?
  - Do output signals respond to the correct input signals in all modules? Is data presentation to operators still correct?
  - Will commands from operator's stations still be executed correctly?
  - Is the communication functioning correctly, peer-to-peer, to host computer, to operator's stations, to printer, etc.?
  - Is there a temporary loss of operation in any of the modules?
– Did the system report the fault?
  - Automatically, or within a certain period of time?
  - Automatically, after a periodic test?
  - At which level of the system was the fault reported (operator's stations, other element)?
– Did the system provide protective measures to avoid the occurrence of the failure?
  - Is fault propagation prevented?
  - Does the operation continue via a redundant path?
  - Are the tasks of the system degraded?
  - Is the operation continued via back-up facilities; does this degrade the system task(s)?
  - Does the output reach a predefined level in case of the inability of the system to continue correct operation?
– Is on-line repair possible without affecting the system task(s)?
  - Is a fault reported by providing unambiguous information on the failed part?
  - Can defective part(s) be exchanged without affecting or interrupting the operation of other modules or elements of the system?
  - Is the repaired or spare module or element automatically started and functioning correctly after reinsertion in the system?

D.4 Interpretation of the results

To ease the interpretation of the results, the percentage of induced faults is calculated for which:

– the behaviour is correct;
– the signalization is correct.

Although the data cannot be used in an absolute manner, it is of value in comparative situations.

A similar approach is followed for the availability assessment, where the self-testing coverage is calculated as the percentage of faults detected by self-testing.

Annex E
(informative)

Available failure rate databases

E.1 Databases

The following bibliography is a non-exhaustive list, in no particular order, of sources of failure rate data for electronic and non-electronic components. It should be noted that these sources do not always agree with each other, and therefore care should be taken when applying the data.

IEC TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*, Union Technique de l'Éléctricité et de la Communication (www.ute-fr.com). Identical to RDF 2000/Reliability Data Handbook, UTE C 80-810

Siemens Standard SN 29500, *Failure rates of components, (parts 1 to 14)*; Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.

Telcordia SR-332, Issue 01: May 2001, *Reliability Prediction Procedure for Electronic Equipment,* (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06).

EPRD (RAC-STD-6100)*, Electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.

NNPRD-95 (RAC-STD-6200), *Non-electronic Parts Reliability Data*, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.

HRD5, *British Handbook for Reliability Data for Components used in Telecommunication Systems,* British Telecom

Chinese Military/Commercial Standard GJB/z 299B, *Electronic Reliability Prediction*, (http://www.itemuk.com/china299b.html)

ISBN:0442318480, *AT&T reliability manual – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors*, AT&T Reliability Manual, Van Nostrand Reinhold, 1990,.

FIDES:January, 2004, *Reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA*. FIDES is available on request at fides@innovation.net.

IEEE Gold book, *The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems,* provides data concerning equipment reliability used in industrial and commercial power distribution systems. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 IEEE (in the US and Canada) +1 732 981 0060 (outside of the US and Canada), FAX: +1 732 981 9667 e-mail: customer.service@ieee.org.

IRPH ITALTEL, *Reliability Prediction Handbook* – The Italtel IRPH handbook is available on request from: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy. This is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed.

PRISM (RAC / EPRD), The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

E.2 Helpful standards concerning component failure

The following standards contain information with regard to component failure.

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

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

IEC 60319, *Presentation and specification of reliability data for electronic components*

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

IEC 60721-1, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*

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

IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

NOTE See Annex D for further information on failure modes of electrical/electronic components.

Annex F
(informative)

Security considerations

F.1 Physical security

Physical security strives to prevent accidental or delibrate destruction by people with access to the equipment. The proposed BPCS should be assessed for its ability to support physical security.

Common physical security assessment points include:

1) access to open data ports on PCs, for example USB, Ethernet, modems, serial ports, etc;
2) equipment placement, for example in cabinets or on tables;
3) access to material within a cabinet, for example key locks, special tools, or simple unlocked latch;
4) access to data about the enclosed equipment, for example temperatures, humidity, and corrosion;
5) access to rack rooms, for example secured entry, monitored space;
6) controls for data changes through the HMI, for example keylocks.

F.2 Cyber-security

F.2.1 General

Although BCS vendors should provide support for cyber-security (including the elimination of known vulnerabilities), ultimately the responsibility for security in operation falls to the user of the equipment.

ISO IEC 27001 and ISO IEC 27002 provide the basis for all cyber-security standards. ISO IEC 27001:2013, Annex A contains eleven clauses numbered from 5 to 15 which provide an outline of what needs to be done. These clauses are by no means exhaustive and an organization may consider that additional control objectives and controls are necessary.

F.2.2 Security policy

The assessment of the cyber-security capabilities of a system should be done within the context of the user's security policy. The security policy should be incorporated into the systems requirements document described in IEC 61069-2 by reference.

Security policies are created to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

F.2.3 Other considerations

ISO IEC 27001:2013, Clause A.10 lists a number of areas against which the applied system should be assessed. For example, the system should be assessed as to how well it supports:

- business continuity management;
- change management, for example ability to document changes and roll them back;
- segregation of duties (roles) and access (permissions), for example supervisor vs. operator; engineer vs. maintenance;

- system planning and acceptance;
- protection against malicious and mobile code, for example anti-virus, anti-spyware, firewalls, patch management, OS upgrades, whitelists, blacklists, etc;
- back up and restore, for example automatic or manual, full or incremental, local or networked, etc;
- media handling, for example open access to all removable media vs. all media ports locked down vs. intelligent handling (only USBs from certain vendors);
- monitoring, for example intrusion protection, intrusion detection, machine health including update status, etc.;
- access control and user management, for example support for which identifiers (something owned (cards), something known (passwords), or something you are (bio signatures), account management (creation, deletion), etc.;
- network access control, for example documented IP ports, firewalls on the network, Ethernet connections disabled when not specifically required;
- operating system access control, for example control of access to command line utilities;
- the consideration of significantly different OS for the BCS from the office systems in the plant to minimise the risk of viruses functioning;
- application and information access control, for example limiting access to certain process control applications to specific roles and limiting non-process control applications to even fewer people;
- mobile computing and teleworking, for example security of the wireless connection, access to mobile devices, control of the applications on the mobile devices;
- cryptographic controls, for example disk drive encryption, message encryption, etc.
- security in development and support processes, i.e., does the vendor have a define security design lifecycle policy and is it followed;
- technical vulnerability management;
- information security incident management;
- business continuity management;
- compliance with legal requirements.

Bibliography

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

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at http://www.electropedia.org)

IEC 60050-192:2015, *International Electrotechnical Vocabulary – Part 192: Dependability*

IEC 60068 (all parts), *Environmental testing*

IEC 60605-1:1978, *Equipment reliability testing – Part 1: General requirements*[1]

IEC 60605-2:1994, *Equipment reliability testing – Part 2: Design of test cycles*

IEC 60605-3 (all parts), *Equipment reliability testing – Part 3: Preferred test conditions*[2]

IEC 60605-4:2001, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60605-6:2007, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

IEC 60605-7:1978, *Equipment reliability testing – Part 7: Compliance test plans for failure rate and mean time between failures assuming constant failure rate*[3]

IEC 60706-4, *Guide on maintainability of equipment – Part 4: Section 8: Maintenance and maintenance support planning*[4]

IEC 60801 (all parts), *Electromagnetic compatibility for industrial-process measurement and control equipment*[5]

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61069-6, *Industrial-process, control measurement and automation – Evaluation of system properties for the purpose of system assessment – Part 6: Assessment of system operability*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

---

1 This publication was withdrawn and replaced by IEC 60300-3-5:2001.

2 This series was withdrawn.

3 This publication was withdrawn and replaced by IEC 61124:1978.

4 This publication was withdrawn and replaced by IEC 60300-3-14.

5 This series was withdrawn.

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61165, *Application of Markov techniques*

IEC 61326 (all parts), *Electrical equipment for measurement, control and laboratory use – EMC requirements*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC TS 62603-1, *Industrial process control systems – Guideline for evaluating process control systems – Part 1: Specifications*

ISO IEC 14764, *Software Engineering – Software Life Cycle Processes – Maintenance*

USA Military Standardization Handbook MIL-HDBK-217 issues A through F, *Reliability prediction of electronic equipment*

_____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.