BS EN 60987:2015

BSI Standards Publication

Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 60987:2015. It is identical to IEC 60987:2007, incorporating amendment 1:2013. It supersedes BS EN 60987:2009 which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by [A1] ⟨A1⟩.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

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 2015

ISBN 978 0 580 86300 4

ICS 27.120.20; 35.240.99

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 30 April 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60987

February 2015

ICS 27.120.20

Supersedes EN 60987:2009

English Version

Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems (IEC 60987:2007 + A1:2013)

Centrales nucléaires de puissance - Instrumentation et contrôle-commande importants pour la sûreté - Exigences applicables à la conception du matériel des systèmes informatisés
(IEC 60987:2007 + A1:2013)

Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme
(IEC 60987:2007 + A1:2013)

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 60987:2015 E

Foreword

This document (EN 60987:2015) consists of the text of IEC 60987:2007 + A1:2013 prepared by SC 45A “Instrumentation, control and electrical systems of nuclear facilities” of IEC/TC 45 “Nuclear instrumentation".

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) 2016-02-16
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2018-02-16

This document supersedes EN 60987:2009.

As stated in the nuclear safety directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law. In a similar manner, this European standard does not prevent Member States from taking more stringent nuclear safety measures in the subject-matter covered by this standard.

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 60987:2007 + A1:2013 was approved by CENELEC as a European Standard without any modification.

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

IEC 61226	NOTE	Harmonized as EN 61226.

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 60780	-	Nuclear power plants - Electrical equipment of the safety system - Qualification	-	-
IEC 60812	-	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)	EN 60812	-
IEC 60880	-	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	EN 60880	-
IEC 61000	Series	Electromagnetic compatibility (EMC)	EN 61000	Series
IEC 61025	-	Fault Tree Analysis (FTA)	EN 61025	-
IEC 61513	2001 [1)]	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-
IEC 62138	-	Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions	EN 62138	-
IEC 62671	-	Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality	-	-
ISO 2768-1	-	General tolerances - Part 1: Tolerances for linear and angular dimensions without individual tolerance indications	EN 22768-1	-
ISO 2768-2	-	General tolerances - Part 2: Geometrical tolerances for features without individual tolerance indications	EN 22768-2	-

[1)] Superseded by IEC 61513:2011.

Publication	Year	Title	EN/HD	Year
ISO 3951-1	-	Sampling procedures for inspection by variables - Part 1: Specification for single sampling plans indexed by acceptance quality limit (AQL) for lot-by-lot inspection for a single quality characteristic and a single AQL	-	-
ISO 3951-2	-	Sampling procedures for inspection by variables - Part 2: General specification for single sampling plans indexed by acceptance quality limit (AQL) for lot-by-lot inspection of independent quality characteristics	-	-
ISO 9001	-	Quality management systems - Requirements	EN ISO 9001	-
IAEA guide NS-G-1.3	-	Instrumentation and control systems important to safety in nuclear power plants	-	-
IAEA 50-C/SG-Q	1996	Quality assurance for safety in nuclear power plants and other nuclear installations	-	-

CONTENTS

FOREWORD 7
INTRODUCTION 9

1 Scope 11
1.1 General 11
1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment 11
1.3 Applicability of this standard to programmable logic devices development 11
2 Normative references 12
3 Terms and definitions 13
4 Project structure 15
4.1 General 15
4.2 Project subdivision 15
4.3 Quality assurance 15
5 Hardware requirements 16
5.1 General 16
5.2 Functional and performance requirements 17
5.3 Reliability/Availability requirements 18
5.4 Environmental withstand requirements 19
5.5 Documentation requirements 19
6 Design and development 20
6.1 General 20
6.2 Design activities 20
6.3 Reliability 21
6.4 Maintenance 21
6.5 Interfaces 22
6.6 Modification 22
6.7 Power failure 22
6.8 Component selection 22
6.9 Design documentation 22
7 Verification and validation 23
7.1 General 23
7.2 Verification plan 23
7.3 Independence of verification 24
7.4 Methods 24
7.5 Documentation 25
7.6 Discrepancies 25
7.7 Changes and modifications 25
7.8 Installation verification 25
7.9 Validation 25
7.10 Verification of pre-existing equipment platforms 25
8 Qualification 26

9 Manufacturing 26
9.1 Quality assurance 26
9.2 Training of personnel 27
9.3 Planning and organisation of the manufacturing activities 27
9.4 Input data 27
9.5 Purchasing and procurement 28
9.6 Production 29
10 Installation and commissioning 32
11 Maintenance 33
11.1 Maintenance requirements 33
11.2 Failure data 34
11.3 Maintenance documentation 34
12 Modification 35
13 Operation 35

Annex A (informative) Overview of system life cycle 36
Annex B (informative) Outline of qualification 37
Annex C (informative) Example of maintenance procedure 38

Bibliography 39

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED SYSTEMS

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 60987 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1989. This edition includes the following significant technical changes with respect to the previous edition:

- account has been taken of the fact that computer design engineering techniques have advanced significantly in the intervening years;
- update of the format to align with the current IEC/ISO directives on the style of standards;
- alignment of the standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3, which includes as far as possible an adaptation of the definitions;

- replacement, as far as possible, of the requirements associated with standards published since the first edition, especially IEC 61513, IEC 60880, edition 2, and IEC 62138;
- review of the existing requirements and updating of the terminology and definitions.

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

FDIS	Report on voting
45A/662/FDIS	45A/666/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.

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

a) Technical background, main issues and organization of the standard

The basic principles for the design of nuclear instrumentation, as specifically applied to the safety systems of nuclear power plants, were first interpreted in nuclear standards with reference to hardwired systems in IAEA Safety Guide 50-SG-D3 which has been superseded by IAEA Guide NS-G-1.3.

IEC 60987 was first issued in 1989 to cover the hardware aspects of digital systems design for systems important to safety, i.e. safety systems and safety-related systems.

Although many of the requirements within the original issue continue to be relevant, there were significant factors which justified the development of this revised edition of IEC 60987, in particular:

– a new standard has been produced which addresses in detail the general requirements for nuclear systems important to safety (IEC 61513);
– the use of pre-developed system platforms, rather than bespoke developments, has increased significantly.

b) Situation of the current standard in the structure of the IEC SC 45A standard series

The first-level IEC SC 45A standard for computer-based systems important to safety in nuclear power plants (NPPs) is IEC 61513. IEC 60987 is a second-level IEC SC 45A standard which addresses the generic issue of hardware design of computerized systems.

IEC 60880 and IEC 62138 are second-level standards which together cover the software aspects of computer-based systems used to perform functions important to safety in NPPs. IEC 60880 and IEC 62138 make direct reference to IEC 60987 for hardware design.

The requirements of IEC 60780 for equipment qualification are referenced within IEC 60987. For modules to be used in the design of a specific system important to safety, relevant and auditable operating experience from nuclear or other applications as described in IEC 60780, in combination with the application of rigorous quality assurance programmes, may be an acceptable method of qualification.

For more details on the structure of the SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the standard

It is important to note that this standard establishes no additional functional requirements for Class 1 or Class 2 systems (see IEC 61513 for system classification requirements).

Aspects for which special recommendations have been produced (so as to assure the production of highly reliable systems), are:

– a general approach to computing hardware development;
– a general approach to hardware verification and to the hardware aspects of computer system validation.

It is recognized that computer technology is continuing to develop and that it is not possible for a standard such as this to include references to all modern design technologies and techniques. To ensure that the standard will continue to be relevant in future years the emphasis has been placed on issues of principle, rather than specific hardware design technologies. If new design techniques are developed then it should be possible to assess the suitability of such techniques by adapting and applying the design principles contained within this standard.

The scope of this standard covers digital systems hardware for Class 1 and Class 2 systems. This includes multiprocessor distributed systems and single processor systems; it covers the assessment and use of pre-developed items, for example, commercial off-the-shelf items (COTS), and the development of new hardware.

d) Description of the structure of the SC 45A standard series and relationships with other IEC, IAEA and ISO documents

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers direct to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common-cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced direct at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not referenced direct by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45A standard series, corresponds to technical reports which are not normative documents.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO 9001 as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA Code on the safety of NPPs and in the IAEA safety series, in particular the requirements of NS-R-1, establishing safety requirements related to the design of NPPs, and Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in NPPs. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED SYSTEMS

1 Scope

1.1 General

This International Standard is applicable to NPP computer-system hardware for systems of Class 1 and 2 (as defined by IEC 61513).

The structure of this standard has not changed significantly from the original 1989 issue; however, some issues are now covered by standards which have been issued in the interim (for example, IEC 61513 for system architecture design) and references to new standards have been provided where applicable. The text of the standard has also been modified to reflect developments in computer system hardware design, the use of pre-developed (for example, COTS) hardware and changes in terminology.

Computer hardware facilities used for software loading and checking are not considered to form an intrinsic part of a system important to safety and, as such, are outside the scope of this standard.

NOTE 1 Class 3 computer-system hardware is not addressed by this standard, and it is recommended that such systems should be developed to commercial grade standards.

NOTE 2 In 2006 the development of a new standard to address hardware requirements for “very complex” hardware was discussed within IEC SC 45A. If such a standard is developed then that standard would be used for the development of “very complex” hardware in preference to IEC 60987.

1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment

Although the primary aim of this standard is to address aspects of new hardware development, the processes defined within this standard may also be used to guide the assessment and use of pre-developed hardware, such as COTS hardware. Guidance has been provided in the text concerning the interpretation of the requirements of this standard when used for the assessment of such components. In particular, the quality assurance requirements of 4.3, concerning configuration control, apply.

Pre-developed components may contain firmware (as defined in 3.8), and, where firmware software is deeply imbedded, and effectively “transparent” to the user, then IEC 60987 should be used to guide the assessment process for such components. An example of where this approach is considered appropriate is in the assessment of modern processors which contain a microcode. Such a code is generally an integral part of the “hardware”, and it is therefore appropriate for the processor (including the microcode) to be assessed as an integrated hardware component using this standard.

Software which is not firmware, as described above, should be developed or assessed according to the requirements of the relevant software standard (for example, IEC 60880 for Class 1 systems and IEC 62138 for Class 2 systems).

1.3 Applicability of this standard to programmable logic devices development

I&C components may include programmable logic devices that are given their specific application logic design by the designer of the I&C component, as opposed to the chip manufacturer. Examples of such devices include complex programmable logic devices (CPLD) and field programmable gate arrays (FPGA).

While the programmable nature of these devices gives the development processes used for these devices, some of the characteristics of a software development process and the design processes used for such devices, are very similar to those used to design logic circuits implemented with discrete gates and integrated circuit packages. Therefore, the design processes and design verification applied to programmable logic devices should comply with the relevant requirements of this standard (i.e. taking into account the particular features of the design processes of such devices). To the extent that software-based tools are used to support the design processes for programmable logic devices, those software tools should generally follow the guidance provided for software-based development tools in the appropriate software standard, i.e. IEC 60880 (Class 1 systems) or IEC 62138 (Class 2 systems).

2 Normative references

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

IEC 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

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

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

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

IEC 61025, *Fault tree analysis (FTA)*

IEC 61513:2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

〈A1〉 IEC 62671, *Nuclear power plants − Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

ISO 2768-1, *General tolerances − Part 1: Tolerances for linear and angular dimensions without individual tolerance indications*

ISO 2768-2, *General tolerances − Part 2: Geometrical tolerances for features without individual tolerance indications*

ISO 3951-1, *Sampling procedures for inspection by variables − Part 1: Specification for single sampling plans indexed by acceptance quality limit (AQL) for lot-by-lot inspection for a single quality characteristic and a single AQL*

ISO 3951-2, *Sampling procedures for inspection by variables − Part 2: General specification for single sampling plans indexed by acceptance quality limit (AQL) for lot-by-lot inspection of independent quality characteristics* 〈A1〉

ISO 9001, *Quality management systems – Requirements*

IAEA NS-G 1.3, *Instrumentation and control systems important to safety in nuclear power plants*

IAEA 50-C/SG-Q:1996, *Quality assurance for safety in nuclear power plants and other nuclear installations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61513, as well as the following, apply.

3.1
ATE
automated test equipment

3.2
COTS
commercial off the shelf; COTS is a subset of pre-developed products

3.3
diversity
existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common cause failure. It may be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways

[IEC 60880:2006, definition 3.14]

NOTE This definition is wider than that used by the IAEA NS-G-1.3 which is as follows: “The presence of two or more systems or components to carry out an identified function, where the different systems or components have different attributes so as to reduce the possibility of common mode failure”. [IEC 61226:2005, definition 3.5]

3.4
firmware
software which is closely coupled to the hardware characteristics on which it is installed. The presence of firmware is generally “transparent” to the user of the hardware component and, as such, may be considered to be effectively an integral part of the hardware design (a good example of such software being processor microcode). Generally, firmware may only be modified by a user by replacing the hardware components (for example, processor chip, card, EPROM) which contain this software with components which contain modified software (firmware). Where this is the case, configuration control of the hardware components by the users of the equipment effectively provides configuration control of the firmware. Firmware, as considered by this standard, is effectively software that is built in to the hardware

3.5
FMEA
failure modes and effects analysis

3.6
FTA
fault tree analysis

3.7
NPP
nuclear power plant

3.8
pre-developed
item which already exists, is available as a commercial or proprietary product, and is being considered for use in a computer-based system

NOTE This definition is consistent with the definition of pre-developed software provided by IEC 61513:2001.

3.9
qualified life
period for which a structure, system or component has been demonstrated, through testing, analysis or experience, to be capable of functioning within acceptance criteria during specific operating conditions while retaining the ability to perform its safety functions in a design basis accident or earthquake

[IAEA Safety Glossary:2006]

3.10
revealed hardware failure
a hardware failure which is detected automatically and reported, for example, a board failure where a watchdog circuit automatically detects the failure and raises an alarm

3.11
safety-related system
system important to safety that is not part of a safety system

[IAEA Safety Glossary:2006]

3.12
safety system
system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[IAEA Safety Glossary:2006]

3.13
single failure
failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

[IAEA Safety Glossary:2006]

3.14
single failure criterion (SFC)
criterion (or requirement) applied to a system such that it is capable of performing its safety task in the presence of any single failure

[IAEA Safety Glossary:2006]

3.15
systems important to safety
system that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

[IAEA Safety Glossary:2006]

3.16
system validation
confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

[IEC 60880:2006, definition 3.42]

3.17
unrevealed hardware failure
hardware failure which is not detected by a system automatically and which only becomes apparent when an attempt is made to use a function which depends upon the failed hardware. Such failures may be discovered by functional testing or when an operational demand is placed upon the system

3.18
verification
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity (ISO 12207)

[IEC 62138:2004, definition 3.35]

4 Project structure

4.1 General

A project established to produce a computer-based system important to safety should be divided up into a number of phases. Each phase should be to some extent self-contained but will depend on other phases for input and will, in turn, provide outputs for other phases. The various project phases together are considered to form the overall safety life cycle (see IEC 61513, Clause 5, which provides requirements for system life cycles). IEC 61513 allows project phases to be performed in parallel providing the integrity of the development process is not compromised.

A quality assurance plan shall be applied to the hardware production process.

4.2 Project subdivision

The following general requirements define the hardware development life-cycle requirements for computer-based systems within the scope of this standard.

a) The hardware development life cycle shall be compatible with the whole system life cycle (Annex A).
b) Each sub-phase of the hardware development life cycle shall consist of well-defined and documented activities.
c) Pre-existing hardware products (for example, COTS) to be included in the design shall be checked, verified and tested as appropriate before use.
d) Adequate means (i.e. spare parts, devices for test and maintenance, etc.) and accommodation (i.e. laboratories, workshops, space, etc.) shall be provided to carry out the tasks associated with each development phase.
e) Each development phase shall include the production of appropriate documentation.
f) Each development phase shall be concluded by performing verification (see Clause 7).
g) Every verification activity shall result in auditable records documenting the conclusions reached and any design changes resulting from the verification performed.
h) All work activities shall be scheduled to ensure that adequate time is allowed for the following:
    1) the resolution of any interactions between the hardware and software development phases required to ensure system hardware/software compatibility;
    2) the production of documentation, and the performance of testing, verification and quality assurance activities.

4.3 Quality assurance

The design and development process shall meet the relevant requirements of IAEA 50-C/SG-Q (compliance with ISO 9001 is one acceptable method of meeting these requirements). A

hardware quality assurance plan shall exist either as a separate document (or documents) or as part of an overall quality assurance plan. The plan shall address the use of pre-existing hardware and the development of hardware as required. All hardware quality-related activities to be performed by the plant operator, owner, contractors and subcontractors as part of the hardware development process should be included in the quality assurance plan.

4.3.1 The plan should address the following phases, as they are applicable to any particular system or development:

a) design and development;

b) procurement;

c) manufacturing;

d) construction and commissioning;

e) operation and maintenance.

4.3.2 It is not a requirement that all the phases listed above be addressed before the design process begins, but, before each phase is initiated, a plan addressing the requirements of that phase shall be in place.

4.3.3 The quality assurance plan(s) should describe the organization, management and execution of quality related activities, including, as relevant:

a) documentation configuration control;

b) the design process;

c) the procurement process for goods and services;

d) configuration control of build instructions, build procedures and drawings;

e) configuration control of materials and items to be used to build the system hardware;

f) quality control activities, such as formal inspections;

g) control of test equipment;

h) control of hardware handling/storage/shipping;

i) the testing process;

j) monitoring of nonconformances raised and the implementation of corrective actions;

k) the procedure for storing quality assurance records;

l) the procedure for internal audits.

5 Hardware requirements

5.1 General

5.1.1 The hardware requirements shall be consistent with the requirements of the system and form part of the computer-system specification (see IEC 61513:2001, Clause 6). The computer-system specification is a description of the combined hardware/software system and states the design objectives for the system and the functions to be performed by the computer system (systems may be developed for a particular application or may be developed generically, i.e. platform development, in which case development is based upon derived generic system requirements).

5.1.2 The hardware requirements shall be specified in the system hardware requirements specification, or in some other suitable document.

5.1.3 Hardware requirements shall be presented according to a technique or method whose format shall not preclude readability, i.e. the hardware requirements should not be difficult to understand.

5.1.4 Functional hardware requirements shall be unambiguous, testable and/or verifiable and achievable.

5.1.5 The hardware requirements specification should give an overview of hardware requirements, identify the hardware functions important to nuclear safety (however, if these are provided in combination with the system software they should be defined in the system requirements specification), identify the hardware design requirements, state hardware reliability requirements, and state the hardware environmental withstand requirements.

5.1.6 The hardware requirements for computer systems may include requirements which are applicable to hardware in general as well as requirements which are particular to computer system hardware (for example; cabling, surface preparation of enclosures).

5.1.7 The hardware functional requirements should generally describe what has to be done and not how it has to be done. However, the use of pre-existing components/platforms may result in a degree of bottom-up hardware design. Before such pre-existing components are selected for use, an assessment shall be performed to confirm that the hardware performance characteristics (for example; failure modes) are consistent with system requirements. If any anomalies are found then these shall be reconciled, either by modifying the hardware design or the system design (while ensuring that system nuclear safety requirements are not compromised).

5.2 Functional and performance requirements

5.2.1 The hardware functional and performance requirements shall be consistent with the functional and performance requirements of the system important to safety.

5.2.2 The hardware functional and performance requirements, combined with the software requirements (to the extent necessary to address all hardware requirements), shall be verified for compliance with the system requirements.

5.2.3 All parts of the system, down to the component level, which contain software shall be assessed as described in 1.2 of this standard.

a) The hardware functional requirements shall include, but are not restricted to, the definition of
   1) the purpose of the overall computer system hardware and of each hardware sub-system;
   2) the numbers and types of sensors and actuators to be connected to the computer system;
   3) the numbers and types of devices for the man/machine interface such as displays, printers and keyboards.

b) Each component or subsystem delivered by a supplier, and which is to be integrated into the system, should be accompanied by a specification which addresses all safety-related aspects of the performance of that item. If such a specification is not provided, then an analysis shall be performed to determine the hardware design characteristics of the component to the extent necessary to confirm its suitability.

c) The hardware performance requirements shall include (as applicable to any particular application)
   1) required data acquisition rate;
   2) required data handling capability;
   3) required computational capacity;

4) required reliability/availability;
5) required communications interfaces (protocols, transmission speeds);
6) required computational and conversion accuracy;
7) required signal noise rejection capability;
8) required response times;
9) physical size limitations;
10) geographic requirements (for example, length of data transmission lines);
11) required level of spare capacity (if required);
12) environmental withstand qualification requirements;
13) electrical power supply requirements.

d) Any constraints imposed upon the hardware design by the system or software design shall be stated.

5.3 Reliability/Availability requirements

5.3.1 The hardware reliability/availability requirements shall be consistent with the overall reliability requirements of the system. They shall include a description of any types of failure which have to be tolerated without loss, or with a defined limited loss, of function. Hardware reliability targets should be provided.

NOTE Hardware reliability in this context is concerned with random hardware failures and excludes any consideration of failures due to logical design errors.

5.3.2 Irrespective of the hardware reliability/availability requirements, the overall I&C architecture for a NPP shall meet the IAEA NS-G-1.3 single failure criteria (see 3.6).

5.3.3 The hardware requirements should give target figures for the hardware reliability parameters (such as mean time between failure (revealed), mean time between failure(unrevealed), mean time to repair (for revealed failures)). Any requirement for reliability claims to be supported with detailed analysis of the hardware design should be stated, for example, subunit, card-level or component-level analysis.

5.3.4 The methods which may be used to analyse the reliability and the effects of system hardware failures include

– FTA, which is concerned with the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event (see IEC 61025 for advice concerning this technique);
– FMEA, which identifies failures which have significant consequences affecting the system performance, for example, reliability, safety, availability (see IEC 60812 for advice concerning this technique).

Where relevant, a suitable analysis technique shall be applied to Class 1 and Class 2 hardware systems to ensure that any potential hardware failures do not have unacceptable nuclear safety effects.

5.3.5 A technique such as FTA when combined with known component failure data may be used to provide calculated values for system hardware reliability characteristics. Such an approach shall be used to analyse the hardware of Class 1 systems (see IEC 61513), unless sufficient operating experience is available to give high confidence that the target hardware reliability targets will be achieved. Such a technique should also be applied for Class 2 systems, or, alternatively, a justification of adequate reliability provided on the basis of qualitative reasoning (for example, quality of components, hardware redundancy, operating experience, proportion of revealed hardware failures versus unrevealed hardware failures, etc.), particularly if hardware reliability requirements are not overly demanding.

5.3.6 Strategies and provisions to assure reliability and availability over the lifetime of the computer system shall be defined. These measures shall be documented as maintenance requirements. They shall include requirements to prevent maintenance activities introducing faults which may lead to common-cause failures. Maintenance activities on multiple train systems are generally considered to be the most likely means of introducing such faults and therefore systems shall be designed to reduce the necessity for such activities to the extent practical. Where maintenance activities having the potential to result in common-cause failures are required, then the design requirements shall specify how the risk of such failures shall be minimized.

5.3.7 Maintenance requirements should address (as applicable to any particular system)

a) requirements for system operation during hardware maintenance activities;

b) consumable replacement, for example, air filters;

c) any requirements for the regular replacement of subsystems, modules and/or components;

d) the extent of hardware revalidation (for example, testing) required following hardware maintenance activities.

5.3.8 However, given that the requirements specification should define “what”, rather than “how”, it may not be practicable to define maintenance requirements in detail at the requirement specification phase of a project, in which case these requirements should be fully defined at a later phase of the development process.

5.4 Environmental withstand requirements

5.4.1 The hardware environmental withstand requirements shall address physical constraints, climatic, seismic, chemical, electrical and radiation conditions as applicable. Any particular requirements applicable during installation and commissioning should also be included.

5.4.2 The degree of immunity to electromagnetic interference shall be specified as required by the operational environment, and tested according to applicable standards, for example, IEC 61000. The electromagnetic operational environment could potentially be affected by a wide variety of electrical interference sources, for example, switchgear, mobile phones, relays, walkie-talkies, electrostatic discharges, lightning, earth faults.

5.4.3 The electromagnetic qualification levels specified should be in accordance with realistic estimates of the operational conditions under all credible worst-case circumstances.

5.4.4 The hardware requirements shall identify any prohibited construction materials and any requirements for particular materials to be used, or for particular types of production processes.

5.4.5 If a particular hardware qualification process is required, then this should be documented in the hardware requirements.

5.5 Documentation requirements

The hardware documentation requirements shall be specified as part of the documentation requirements of the computer system (see IEC 61513). The documentation to be produced should include (as relevant):

a) design documents (system hardware components, hardware design of interfaces, etc.);

b) operators' manuals;

c) maintenance manuals.

6 Design and development

6.1 General

This clause is applicable to system, subsystem and module level hardware design and development.

6.1.1 The design and development process for new hardware should take as an input the hardware requirements specification. The design process should progress through various design stages which result in the production of hardware which meets the hardware requirements specification.

6.1.2 The more general level of design activity may be termed the “preliminary” design, consisting of the analysis of different design alternatives in order to define the hardware system architecture in terms of subsystems and modules.

6.1.3 Preliminary design is generally followed by one or more detailed design levels. The detailed design activities shall expand the preliminary design to address the detailed design of subsystems, modules and components to the extent that the overall hardware design description is sufficiently complete to be implemented.

6.1.4 Prototype hardware may be built, not only to demonstrate successful interaction between hardware modules, but also to check hardware and software compatibility.

6.1.5 Pre-developed (for example, COTS) components could be used for all system hardware or for a subset of hardware components. Subclauses 6.2 to 6.7 mainly consider the situation where bespoke hardware development is required; however, where appropriate, guidance is also provided which defines how the requirements of these subclauses may be applied to the use of pre-developed components.

6.2 Design activities

6.2.1 System performance requirements which are dependant upon hardware performance shall be addressed by the hardware design, and evidence shall be made available, either through analysis or testing, to show that the hardware design meets these requirements. Such requirements may include calculation accuracy, time response, environmental withstand capabilities and electrical supply requirements (for pre-existing components, the component hardware specification shall be verified against the system hardware requirements to ensure that the pre-existing components meet the specified requirements, or hardware performance shall be verified by test).

6.2.2 Any discrepancies against hardware requirements shall be reconciled, by either changing the design or changing the requirements (the impact of any changes shall be fully assessed and documented).

6.2.3 The hardware designers shall identify such tests as are necessary to show that the required performance has been achieved. Such tests may be performed on the hardware alone, or performed when the hardware is integrated with the software, i.e. as part of the system integration testing phase.

6.2.4 The hardware designers shall specify any maintenance activities required to provide confidence that the performance and reliability requirements are achieved during the full operational life of the equipment. These may include operational tests, calibration, repair, periodic replacement and maintenance procedures. Such activities should be performed to an extent which provides sufficient confidence in correct operation of the equipment and yet reduces human interference and the performance of intrusive work with the systems to a minimum, so as to reduce the likelihood of faults (such as potential common-mode failure faults) being introduced through maintenance activities.

6.2.5 Where a qualified target life is specified, justification shall be provided that this target is realistic and achievable.

6.3 Reliability

6.3.1 Reliability requirements should be specified in the hardware requirements documentation (see 5.3).

6.3.2 As required to support the system-level safety analysis, an analysis of the potential for hardware failures shall be made during design. Where multiple trains of a system or multiple systems (each of which may have a single or multiple trains of equipment) are used to implement a nuclear safety function then proper consideration of the potential for common-cause hardware failures shall be included in this analysis. Potential means of hardware based common-cause failure are as follows:

– maintenance activities performed simultaneously or sequentially on multiple trains of equipment (particularly where such activities may introduce unrevealed hardware faults);
– periodic testing;
– coincident unrevealed random hardware failures on multiple trains of equipment which affect the same nuclear safety function(s);
– latent design faults affecting multiple equipment trains, and which were not revealed by the design process.

6.3.3 Methods which may be used to analyse hardware reliability and the effects of system hardware failures include FTA and FMEA (see 5.3.4).

6.3.4 The hardware design should minimize the potential impact on nuclear safety of the following factors:

– maintenance activities;
– system failure due to random hardware failure;
– hardware failure due to environmental conditions.

6.3.5 If the estimated hardware reliability is considered to be inadequate for a particular role then compensating actions shall be taken. These may take the form of design improvements or operational changes (such as an increase in the frequency of operational testing). However, care should be taken when the option of increased operational testing is chosen, as any intrusive activities on operational plant carries an intrinsic degree of risk as faults may be induced or introduced (i.e. the net overall effect upon safety of operational testing may be negative). Ideally, all testing should be performed when potential faults in the testing process would not have a nuclear safety impact, for example, during station outages or when the equipment to be tested is isolated from operational plant.

6.3.6 Where a probabilistic safety assessment is used to support the safety case of an NPP, the estimated probabilistic hardware reliability values (for example, as developed from FTA) may be fed into the NPP analysis, and so contribute to the accuracy of the overall station reliability calculations.

6.4 Maintenance

The hardware design shall address any specific maintenance requirements contained within the hardware requirements specification. In addition, where practicable, the design should include features to reduce the risk of faults being introduced due to maintenance activities; examples of such features are as follows:

– components that may require replacement due to failure should be easily accessible;

– replaceable components should be clearly identified so that maintenance staff may easily check that the correct components are used;
– there should be adequate spacing of terminals;
– there should be adequate provision of dedicated terminals for use during calibration/testing activities (so that plant wiring does not have to be disconnected to facilitate such activities);
– hardware design should have a structured layout with clear labelling to reduce the potential for maintenance errors.

6.5 Interfaces

IEC 61513, 6.1.1.2.1, provides system interface requirements which aim to prevent the propagation of failures across system interfaces.

6.6 Modification

To the extent required by the hardware requirements specification, the hardware shall be designed to be capable of being modified (see Clause 12).

6.7 Power failure

To the extent required by the hardware requirements specification, the computer system shall be designed to be insensitive to the consequences of short-term power failures and to potential variations of the power supply (voltage/frequency). System features shall be provided to notify operators and maintenance staff of such power fluctuations (this role may not be allocated to hardware, and hence may be out of scope of this standard).

6.8 Component selection

Where pre-existing components are to be used, the design of the components shall be compatible with their role within the system hardware.

6.9 Design documentation

6.9.1 The hardware design documentation shall describe the hardware design and the means by which the hardware requirements have been addressed. Standardized forms of design documentation and the use of automated hardware design tools are recommended.

6.9.2 A hierarchy of design documents addressing the computer system hardware should be produced which consist of a number of documentation ‘levels’. The design documentation at each level should specify the design aspects relevant to that level and define the hardware requirements for the lower levels. Documents (as applicable) for manufacturing/assembly, factory testing, installation, commissioning, maintenance and operation shall be produced during the design process.

6.9.3 A preliminary hardware design description may be produced which defines the hardware architecture, i.e. the structure and relationship between the different parts of the system. It should include the general layout of hardware, with block diagrams of the subsystems and modules of the lower levels. It should also include hardware requirements for the detailed design, such as:

– the number and types of central processor units and other processors;
– computer memory hardware requirements;
– the number and types of interfaces;
– the number and types of data links and busses.

6.9.4 At the conclusion of the design and development of the hardware, documentation shall be produced which contains a full and final description that conveys both the design details down to the lower level and the capabilities, limitations and other characteristics of the hardware.

6.9.5 This final description documentation shall provide the following information:

a) a design overview;

b) cross-references to supporting design documents;

c) a description of the subdivision of the hardware in terms of hardware subsystems;

d) a description of each subsystem in terms of its major modules and components (using for example, block diagrams, circuit diagrams);

e) a description of subsystem hardware interfaces. Interfaces shall be described as appropriate in logical, physical, electrical or other terms;

f) a description of the computer system hardware interfaces. Interfaces with any other systems either within or outside the nuclear plant, shall be identified showing the specific interfaces and related hardware requirements;

g) the physical layout – a description with diagrams of the physical layout of the equipment should be provided;

h) qualification data (see Clause 8), including the definition of any necessary actions (such as exchange of components) required to maintain the specified qualification lifetime. Qualification data relevant to shelf life of spare parts should also be provided where relevant;

i) maintenance requirements;

j) a description of how the requirements for hardware reliability and fail-safe properties are fulfilled.

7 Verification and validation

7.1 General

7.1.1 The design and development process shall include formal checks that the hardware design deliverables from each phase of design and development meet the requirements imposed by the previous phase.

7.1.2 The hardware verification process is generally considered to begin with the verification of the hardware design requirements against the system design requirements, and is considered to be complete when the system software is integrated into the hardware. For Class 1 and Class 2 systems, IEC 60880 and IEC 62138, respectively, provide relevant requirements for the hardware/software integration phases.

7.2 Verification plan

A formal verification plan shall be prepared to define the approach to be used to verify the hardware design and to control the verification process. The plan shall be prepared prior to initiating verification actions. The plan (or plans) should document the personnel/organization to be used, organizational structure, verification methods to be used, level of verification to be performed, schedules and other significant project activities related to verification.

a) Verification may be performed in parallel with the design process (providing adequate configuration control arrangements are in place) so that errors may be detected and corrected as soon as possible.

b) Formal verification actions shall not take place until design components are released for verification by the design personnel. Once released for verification, the design and related documentation shall be maintained under formal configuration control.

c) After release for verification, the design change process shall ensure that all subsequent changes to the hardware design are adequately verified (i.e., as required by 7.7).

7.3 Independence of verification

7.3.1 For Class 1 hardware design, verifiers should be managerially independent from the hardware designers; for example, they may be in different departments of the same organization or from a different organization. For Class 2 systems, verifiers shall not have designed the items to be verified; however, persons involved with verification may be from the same organization as the individuals responsible for the design. In addition to these requirements:

a) the verification personnel shall be technically competent;

b) any verification findings and responses to those findings by the design team shall be formally documented;

c) verification shall be performed according to documented procedures.

7.3.2 For Class 2 hardware development where ATE is used to verify the correctness of hardware, then the detailed independence requirements defined above apply to the personnel who design the ATE, rather than the personnel monitoring the performance of the tests being performed by the ATE. However, for the development of all Class 1 hardware, individuals shall not be responsible for performing tests (with or without ATE) on hardware components which they have designed.

7.4 Methods

Critical reviews, audits, analysis, manual tests or tests performed using ATE, or a combination of these methods, may be used to provide hardware design verification. The basis for the choice of verification method(s) to be used shall be documented in sufficient detail to allow auditing by personnel who are not directly involved in the design or verification activities.

a) When choosing the appropriate verification method, the following issues shall be considered when relevant:
   - the safety-related classification of the system (i.e. Class 1/2, with Class 1 requiring the most rigorous techniques);
   - the documented reviews and tests which will be performed on the integrated hardware and software as part of the system verification and validation processes, i.e. to eliminate such activities from the hardware verification and validation processes, so as not to inefficiently utilise resources by duplicating work;
   - previous verification activities performed on the hardware or on systems containing the hardware (i.e. where equipment has been effectively pre-qualified);
   - system design characteristics, for example, size, maturity/novelty of design principles used, failure modes and complexity;
   - supporting data which may be available from other sources, such as that obtained from quality assurance and environmental qualification processes.

b) Appropriate tools and methods shall be available to support the testing of subsystems and electronic components to ensure that they can be thoroughly tested. ATE should be used to improve the repeatability and thoroughness of testing where effective.

c) Test instruments used in the verification or testing process shall be calibrated where necessary to confirm accuracy, in which case procedures shall ensure that only calibrated instruments are used.

d) Software-based test tools shall be validated prior to use and shall be placed under configuration control.

e) The results of all formal testing shall be recorded (informal testing may be performed during the design process as a precursor to formal testing). Auditable records of formal

testing shall be available which are sufficient to demonstrate that all tests have been performed, and that any test anomalies have been successfully reconciled.

7.5 Documentation

Auditable records resulting from verification activities shall include the verification programme plan, test procedures, test results, design change records and documentation of any discrepancies which are discovered during the hardware verification process (together with records showing how each discrepancy was reconciled).

a) Test procedures should be clearly written, provide step-by-step instructions for hardware verification and should contain detailed information of the test set-up.

b) Test procedures shall contain unambiguous pass/fail criteria.

c) Test procedures implemented by software shall be documented.

7.6 Discrepancies

Discrepancies found during the verification process shall be formally documented and transmitted to the relevant personnel for resolution. The response shall be formally documented to provide a traceable path to assure that all discrepancies are assessed and any identified design deficiencies corrected or accepted. Where design deficiencies are accepted, all impacts on system documentation shall be fully addressed.

7.7 Changes and modifications

7.7.1 All design changes shall be subject to design impact assessment to determine which documentation requires amendment and what design and verification processes should be repeated.

7.7.2 Modified parts shall be identified in accordance with the relevant quality control procedures.

7.8 Installation verification

Verification of correct system installation shall be in accordance with Clause 10.

7.9 Validation

System validation of the integrated hardware and software shall be performed as required by IEC 61513, IEC 60880 or IEC 62138 as applicable.

7.10 Verification of pre-existing equipment platforms

Where a pre-existing equipment platform is to be used, then the suitability of the platform for its intended use shall be assessed. The assessment process shall consider the following design aspects:

a) design process used to develop the hardware, i.e. assess against the relevant requirements of Clause 6;

b) experience of use (where actual hardware reliability data provides confirmation that hardware reliability targets are achievable, then considerable confidence in the performance of the hardware in the proposed application may be gained). Relevant experience-of-use data which support the required hardware reliability target may be used to compensate for discrepancies in the development methods used, as identified by item a) above;

c) if item a) above does not provide adequate information to justify the hardware for its intended use, then additional work may be performed to support the assessment, for example, testing, analysis, justification.

8 Qualification

IEC 60780 provides requirements concerning the qualification of hardware for nuclear safety applications and the relevant requirements of the standard should be applied. Annex B provides an informative outline of the qualification process.

9 Manufacturing

9.1 Quality assurance

9.1.1 Manufacturing may be one phase of the overall safety life cycle (see 4.1 and 4.2).

Where manufacturing is a phase of the overall safety lifecycle then manufacturing activities shall be included in the hardware quality assurance plan of the overall safety life cycle or, if not, shall be addressed by a separate manufacturing quality assurance plan (see 4.3).

Manufacturing-related activities during the design process (such as manufacturing assessments during product qualification) shall be included in the hardware quality assurance plan of the overall safety life cycle.

Hardware produced during the manufacturing phase, and addressed in this clause, includes individual modules, sub-assemblies or equipment as a whole.

9.1.2 The primary consideration when defining manufacturing processes to which the quality assurance plan applies shall be to ensure that the manufacturing does not compromise the delivery of the safety functions by the product.

9.1.3 Procedures and work instructions shall be established for the manufacturing activities. These activities include manufacturing processes and their control, inspection and testing, independent quality surveillance and inspection, identification, handling, packaging, storage and delivery.

9.1.4 The extent and details of procedures and work instructions necessary for manufacturing activities shall be defined according to the relative importance of the safety functions being performed by the hardware components (the intended system Class).

The objectives of the manufacturing activity are:

– to ensure the manufactured items are identical and meet the product description and specification generated during the design and development phases,
– to ensure the production items meet the requirements demonstrated by the initial model during the qualification programme.

9.1.5 When the hardware contains components provided by external suppliers, the suppliers shall be evaluated and selected based on their ability to manufacture and supply these items in accordance with the design requirements, including the requirements in Clause 9 and appropriate quality assurance program requirements.

In the case where a programmable electronic equipment component is part of the external scope of supply, an assessment of the supplier's ability and willingness to support a successful qualification of the equipment should be performed as part of supplier qualification.

NOTE Specific product selection and qualification criteria may be found, as appropriate, in standards such as IEC 60880, IEC 61513 or in related sub-tier standards such as IEC 62671 and IEC 62566.

9.1.6 When the designer of the I&C system chooses to outsource any process that affects product conformity to requirements, control over such processes shall be ensured. The type and extent of control to be applied to these outsourced processes shall be defined within the quality management plan.

9.1.7 Criteria for the selection, evaluation and re-evaluation of either external suppliers or sub-contractors shall be established (e.g. general information such as business areas, scope of supply, technical capability and manufacturing capacity, quality organization, system and technical audits, financial health, market behaviour, etc.).

9.1.8 Criteria for selection, evaluation and re-evaluation of external products shall be established and these criteria shall be based on the requirements of relevant standards (e.g. IEC 60880, IEC 62671 and/or IEC 62566).

9.1.9 The use of manufacturing processes independently certified to recognised international standards by accredited bodies is recommended (e.g. the International Register for Certificated Assessors scheme for ISO 9001).

9.2 Training of personnel

9.2.1 The necessary competence for personnel performing any kind of work involved in the manufacturing and control activities shall be established, documented and maintained.

9.2.2 If personnel experience, education, and training records do not by themselves fulfil the requirements of 9.2.1, training or relevant other actions shall be provided to achieve the necessary competence. The effectiveness of the training and actions taken shall be evaluated and recorded.

9.2.3 The personnel shall be trained to be aware of the relevance and importance of their activities and how they contribute to the achievement of the quality and safety objectives. In addition, appropriate records of education, training, skills and experience shall be established and maintained.

9.3 Planning and organisation of the manufacturing activities.

9.3.1 As part of the overall project planning (see 4.3), a manufacturing plan shall be established at the start of the project and shall be kept up to date throughout the project.

9.3.2 Interfaces between different groups involved in the design and development shall be managed to ensure effective communication, clear definition of and assignment of responsibility for all aspects of the equipment relevant to the manufacturing process.

9.3.3 Effective arrangements for communicating with customers or inspectors shall be established to define and schedule manufacturing steps and the associated inspections, audits or controls.

9.4 Input data

9.4.1 Manufacturing inputs shall be established during the design and development phase in order to provide appropriate information for purchasing, production and quality controls including product acceptance criteria.

The input data shall include the following information:

– the need for independence between manufacturing activities and the associated processes documented formally;

– any requirements for the customer approval of changes during manufacture to the sourcing of components or manufacturing consumables (e.g. solder);

– any requirements for the customer approval of the substitution during manufacture of components or manufacturing consumables (e.g. solder);

– any special training as a consequence of the equipment having a nuclear application.

9.4.2 Any requirements specified during the design process which have an impact on the manufacturing process shall be taken into account. This includes any statutory or regulatory requirements applicable to the product as well as physical and technical characteristics.

NOTE Commonly used manufacturing standards may be considered based on the safety Class of the functions being performed by the hardware components. (e.g. ISO and ISA manufacturing standards, NEMA enclosures and protections standards, fire ratings standards, material processes standards, wiring techniques standards, etc.).

9.4.3 Input documents shall be reviewed prior to initiating purchasing activities and manufacturing activities. The review shall ensure that product requirements are defined and that the defined requirements can be met. The findings of the review shall be recorded.

9.5 Purchasing and procurement

9.5.1 Purchasing and procurement process

9.5.1.1 Specific purchase requirements shall be established based upon the effect of the purchased product on subsequent product realization or the final product. The requirement shall include a list of documents or access to documents necessary to achieve the qualification of the equipment.

9.5.2 Procurement process of commercially available components

9.5.2.1 Adequate demonstration or other suitable evidence shall be provided, that all the equipment components, including electronic components boards and housings meet the specified requirements (e.g. functionality, environmental withstand, reliability and lifetime).

9.5.2.2 Demonstration shall be provided that the selected components fulfil the expected characteristics.

The demonstration may be based on:

– data provided by the supplier of the components (nature and results of testing after manufacture, feedback, results of periodic tests, audits, approvals know-how, etc.),
– or self-established, formalized and documented feedback obtained through checks performed on successive batches, results of periodic tests conducted on samples, and operating results (such as operating time, failures of components),
– analysis (e.g. circuit level FMEA), component level operating history assessment, design quality assurance process and records, previous product/component certifications or qualifications,
– or results obtained during type test previously performed.

9.5.2.3 Adequate means shall be established to demonstrate the quality of the purchased component. This quality demonstration shall be commensurate with the safety Class of the intended function(s) of the component(s).

NOTE 1 Related means can consist of type tests of the component itself or of a sub-assembly including it.

NOTE 2 The expected quality includes the physical behaviour, static and dynamic electrical behaviour, under normal and extreme environmental conditions as well as the expected reliability.

For programmable electronic equipment, refer to specific product selection and qualification criteria in IEC 60880 and IEC 61513 and its related sub-tier standards such as IEC 62671, or IEC 62566 as appropriate.

9.5.3 Procurement process of parts used in the I&C equipment

9.5.3.1 The type and extent of control applied to the supplier and the purchased product shall be defined and contractually established with the supplier.

When the purchased products consist of programmable electronic components, specific additional requirements shall be in place to ensure strict configuration management and version control on hardware and software revisions as per approved qualification and manufacturing records. Any and all changes shall be reported by the manufacturer and a safety impact assessment provided.

9.5.3.2 Records of the results of evaluations and any necessary actions arising from the evaluation shall be maintained.

9.5.3.3 Purchasing information shall describe the product to be purchased, including, where appropriate:

– technical specification, (e.g. as schematics, drawings, control programs, test programs),
– requirements for approvals (e.g. processes, procedures, product and equipment),
– requirements for qualification of personnel,
– quality management system requirements.

9.5.4 Verification of purchased product

9.5.4.1 Inspection or other activities shall be established and performed to ensure that the purchased product, including the related expected documentation, meets the specified purchase requirements (see 4.2 and Clause 7).

9.5.4.2 Where verification at the supplier's premises is intended to be performed, verification arrangements and verification methods used shall be stated in the purchasing information. Requirements for preparation and acceptance of factory acceptance test plan(s), requirements for supervision and witnessing of acceptance testing, and requirements for final factory surveillance and inspection activities (i.e. to address any previously identified non-conformance issues and to confirm they have been resolved prior to shipment to site) shall be established.

9.5.4.3 The verification arrangements shall contain statements related to follow-up and control steps such as sampling tests, on-site observation or breakpoints.

9.5.4.4 Strict quality control shall be ensured of the incoming goods, including the use of bonded stores where appropriate. The controls on the incoming goods shall include non-intrusive controls (e.g. visual inspection) and, where appropriate, intrusive controls, such as electrical tests and functional behaviour.

9.5.4.5 Dimensional controls and sampling plans for inspection shall conform to those specified in ISO 2768-1, ISO 2768-2, ISO 3951-1 and ISO 3951-2.

9.6 Production

9.6.1 Control of production

9.6.1.1 The overall manufacturing activity shall be defined in a reference process description as part of the overall product life cycle.

9.6.1.2 Production shall be planned and carried out under controlled conditions.

Controlled conditions shall include, as applicable,

– availability of information that describes the characteristics of the product,
– availability of work instructions,
– availability of quality instruction,
– use and availability of suitable equipment and tools,

[A1] – full traceability of component parts,

– full recording of the dates and personnel involved for each production operation,

– implementation of product release, delivery and post-delivery activities.

9.6.2 Specification and control of production environmental conditions

9.6.2.1 Requirements for the environmental conditions for production and control areas shall be defined as necessary.

9.6.2.2 Area access conditions such as rights to enter, procedures to follow and clothing to be worn shall be defined as necessary.

9.6.2.3 Control plans for the environmental conditions of, and the access control to, the manufacturing facilities shall be established (e.g. dust in the atmosphere, creating an inert atmosphere, humidity or temperature regulation, control of chemical composition of water, control of electrostatic discharges).

9.6.3 Validation of processes for production

9.6.3.1 Specific processes for production provision shall be validated where the resulting output cannot be verified by subsequent monitoring or measurement and where, as a consequence, deficiencies become apparent only after the product has been in use or delivered.

9.6.3.2 Validation shall demonstrate the ability of these processes to be robust in order to achieve planned and repeatable results.

Arrangements shall be established for these processes including, as applicable:

– defined criteria for review and approval of the processes,

– approval of equipment and qualification of personnel,

– use of specific methods and procedures,

– requirements for records and validation,

– handling of defective parts including possible consequences for the production process.

9.6.4 Assessment of the manufactured I&C equipment acceptance and reproducibility

9.6.4.1 The equipment produced shall be assessed and stated to be accepted by the customer.

9.6.4.2 The acceptance shall be based on the quality assurance management, the overall hardware qualification process and successful qualification results of the component, modules or equipment which usually are the first of a kind.

9.6.4.3 The designer of the I&C system shall be deemed able to reproduce series equipment identical to the qualified hardware either by means of internal manufacture and assembly, or by means of sub-contract manufacture and assembly.

9.6.4.4 The evaluation of manufacturing should be based on surveys focusing on the I&C system manufacturer's organization and the technical means to manufacture the products.

9.6.4.5 When changes occur after the qualification of the initial item, an impact analysis shall be performed by the designer of the I&C equipment and conclusions shall be evaluated to decide if a new qualification has to be done or if the results of the previous qualification remain unchanged. [A1]

9.6.5 Control of production tools, monitoring and measuring devices

9.6.5.1 The tools necessary to manufacture the product shall be determined.

9.6.5.2 Monitoring and measurement processes to be undertaken on the product shall be determined to provide evidence that the product conforms to its requirements.

9.6.5.3 Processes shall be established to ensure that production, monitoring and measurement are carried out in a manner that is consistent with the production, monitoring and measurement requirements.

9.6.5.4 Where necessary to ensure valid results, tools and measuring devices shall:

– be calibrated or verified, at specified intervals or prior to use, against measurement standards or established basis used for calibration or verification which are recorded;
– be adjusted or re-adjusted when necessary;
– have identification in order to determine their calibration status;
– be safeguarded from adjustments that would invalidate the measurement result;
– be protected from damage and deterioration during handling, maintenance and storage.

9.6.5.5 Quality assurance processes shall ensure that if manufactured equipment is found not to conform to requirements due to faults in the manufacturing process that adequate corrective action is taken.

9.6.5.6 Records of the results of calibration and verification shall be maintained.

9.6.5.7 When software based devices are used in the monitoring and measurement activities, the ability of the device to satisfy the intended application shall be confirmed. This shall be undertaken prior to initial use and reconfirmed as necessary.

NOTE Confirmation of the ability of computer software to satisfy the intended application would typically include its verification and configuration management to maintain its suitability for use.

9.6.6 Identification and traceability

9.6.6.1 The manufactured system shall be identified, as well as the parts and materials used to manufacture the system, by suitable means throughout product realization.

9.6.6.2 The manufactured system status shall be monitored throughout the overall production process.

9.6.6.3 A unique identification of the system, and of the included parts, shall be ensured and records of changes shall be maintained for traceability purposes.

9.6.6.4 An identification file shall be established for each equipment and/or subassembly in order to define the reference model including the description of the equipment, the internal assemblies, components and versions. These files may typically include a list of sub-assemblies, plans, drawings, diagrams, data sheets, references to sub-tier detailed files in order give an exhaustive description of a version of the system and/or sub-assemblies.

9.6.7 Preservation of product

9.6.7.1 The system, and the included parts, shall be preserved during internal processing in order to maintain conformity to requirements. Preservation shall include identification and as applicable, handling, packaging, storage and protection conditions given before the acceptance test of the equipment.

9.6.8 Sustainability of tools and skills

9.6.8.1 Requirements for the maintenance of tools and other means used during the manufacturing, testing, and validation activities shall be defined during the planning of the manufacturing activity and commensurate with the safety class of the functions being performed by the components.

9.6.8.2 Requirements shall be defined for maintaining the skills involved in manufacturing, validation and testing activities.

9.6.9 Resolution and control of non-conformities

9.6.9.1 Non-conformities detected during environmental qualification tests, verification activities or manufacturing shall be identified and recorded according to the quality assurance plan (see 4.3.3).

9.6.9.2 Corrections and solutions shall be identified and recorded in such a way that they can be easily auditable by external parties. The related records shall indicate the nature of the changes, include impact analysis and associated justifications and approval.

9.6.9.3 Controls shall be ensured on the production line to check that the modifications have correctly been taken into account and that controls and test procedures have been correctly adapted (manufacture, identification and acceptance tests).

10 Installation and commissioning

10.1 Packing, handling, transport, storage and unpacking shall be such as to prevent any damage to the system.

10.2 Before the system is unpacked and installed, the environment in which the system is to be installed shall be verified to conform to the hardware environmental requirements, as covered by 5.4.

10.3 Adequate procedures and information shall be available to enable the system to be installed, cabled and wired in accordance with the design requirements; for example, earthing requirements. Identification of items of equipment shall form part of this information. For this purpose, a quality plan shall be applied. The system shall be installed, cabled, tested and set to work in accordance with defined procedures.

10.4 The proper working of the system at site shall be checked by planned and specified commissioning tests, as required by IEC 61513.

10.5 The tests shall be performed in accordance with relevant standards, for example, IEC 61000.

10.6 The severity level of electromagnetic interference tested shall be chosen in such a way that it equals or surpasses the worst estimated conditions to which the system may be subjected while required to operate.

10.7 For Class 1 and 2 systems off-site type testing of electromagnetic interference withstand should be performed. For Class 2 systems this type of testing should generally be considered to provide adequate assurance of correct operation. For Class 1 systems on-site testing should also be performed if practicable and effective.

10.8 On the completion of installation and commissioning, and when it has been confirmed that all acceptance criteria have been addressed (or concessions agreed), ownership of the system may be transferred to the user, as described in IEC 61513.

11 Maintenance

Hardware maintenance comprises

– tests, checks and calibration (which may be either periodic, within specified maximum intervals, or following the replacement, exchange, overhaul or repair of components [i.e. revalidation]);

– maintenance such as is required to maintain the computer hardware in good working order, for example, replacement of expendables, or the preventative exchange or overhaul of equipment, subunits, parts or components;

– repairs, i.e. the restoration of the operability of failed equipment, subunits and parts.

11.1 Maintenance requirements

11.1.1 A formal procedure (or procedures) shall be specified and applied to control the execution and the documentation of maintenance activities (see Annex C).

This shall take into account

– preventative actions required to reduce the potential for faults to be introduced and the potential for personal injuries to occur;

– organizational and operational preparations required if the maintenance activities have the potential to affect plant operation, or the availability of safety functions or safety-related functions.

11.1.2 Maintenance shall be undertaken by qualified and authorized personnel. It shall be performed according to specified procedures. The procedures shall make provision for personal certification (by an authorized person, or by automated test) to the effect that, where tasks may have a direct impact upon safety, each task has been completed satisfactorily.

All relevant information, such as time and date, replacements fitted, etc., shall be recorded.

11.1.3 The records arising from maintenance work shall be made available for audit if required.

11.1.4 For some critical components, rather than performing component replacement only when failure occurs, a preventative maintenance regime may be adopted. In this case, controls should be applied to ensure that components are replaced after a period of time not longer than their qualified life (if applicable, see IEC 60780).

11.1.5 Spare parts held by the operating organization shall be kept in a store which meets any environmental conditions relevant to the parts to be stored there. The shelf life of spare parts shall be controlled and modified as necessary with the passage of time in accordance with the ageing characteristics of the hardware. Any activities needed to preserve the state of readiness of the spares, such as periodic energization, shall be addressed.

11.1.6 Spares should be qualified to a standard equivalent to that used to qualify operational components. Any proposal to reduce the qualification requirements of a Class 1 or 2 system component, or to extend the qualification life of such a component, should be treated as a system modification and assessed as such; see Clause 12 (IEC 61513 specifies the controls to be placed on system modifications).

11.1.7 All spares shall be under configuration control and shall have adequate identification marking or labelling.

11.1.8 It is recommended that the future supply of spare components should be secured to the extent practicable (for example, either through the holding of spares, assurances from suppliers or by having access to manufacturing capability).

11.2 Failure data

11.2.1 Failure data acquired during equipment operation constitutes a major source of information which can be used to improve

– component reliability data knowledge (by taking into account real operating environment conditions);
– equipment reliability evaluations (by determining actual field failure data and by observing availability in operating conditions);
– maintenance policy (through better spare parts optimization, better preventative maintenance schedules and better maintenance personnel training requirements).

11.2.2 Accordingly, field failure data (from information available from maintenance reports) should be logged in a failure data bank.

11.2.3 The maintenance reports shall contain (if relevant and if known)

– identification of the system with the failed component;
– failure circumstances and failure effects;
– failed component identification;
– component location within the system;
– description of the fault which caused the failure;
– date of intervention;
– age of failed component;
– identification of person(s) who raised the report;
– identification of person(s) who diagnosed the fault.

11.2.4 Failure data for systems important to safety shall be subject to periodic review to ensure that the frequency of component failure remains within acceptable limits. Any statistically significant negative trends in the data should be extrapolated to ensure, to the extent practicable, that the equipment will continue to operate satisfactorily in the future period up to the next assessment of the failure data of the equipment, or until the equipment may be replaced (whichever is the shortest period).

11.3 Maintenance documentation

11.3.1 Instructions for maintenance shall be provided in written or electronic form by means of procedures, manuals, handbooks, etc.

11.3.2 Maintenance documents shall describe the hardware maintenance policy for the equipment in use, including identification of hardware components which require regular checking, re-calibration or replacement.

11.3.3 Maintenance documents shall describe any relevant diagnostic processes which should be used to detect the failure of specific modules.

11.3.4 Documentation shall describe the repair policy, i.e.

– the methods of repair or substitution of different subsystems, modules and components;
– any restrictions which the system should be subjected to during repair time (for example, the system or parts of the system which shall be switched off);
– the extent to which equipment shall be revalidated after a repair.

In addition to the procedures for scheduled periodic maintenance, diagnostic procedures should be provided, where relevant and practicable, which may be used to assist in the investigation of anomalous system behaviour and to identify failed components.

12 Modification

Hardware design modification may be required to correct defective performance or to address new or revised performance requirements.

12.1 The process controlling hardware design changes shall be compliant with the requirements of 6.3.6 of IEC 61513:2001.

12.2 Hardware design changes which have an impact beyond a single design phase (i.e. excluding any changes made by the designers while in the process of creating the design) shall be controlled by a documented procedure. This design change procedure should take account of any potential impacts to other aspects of the system design, such as other hardware components and software.

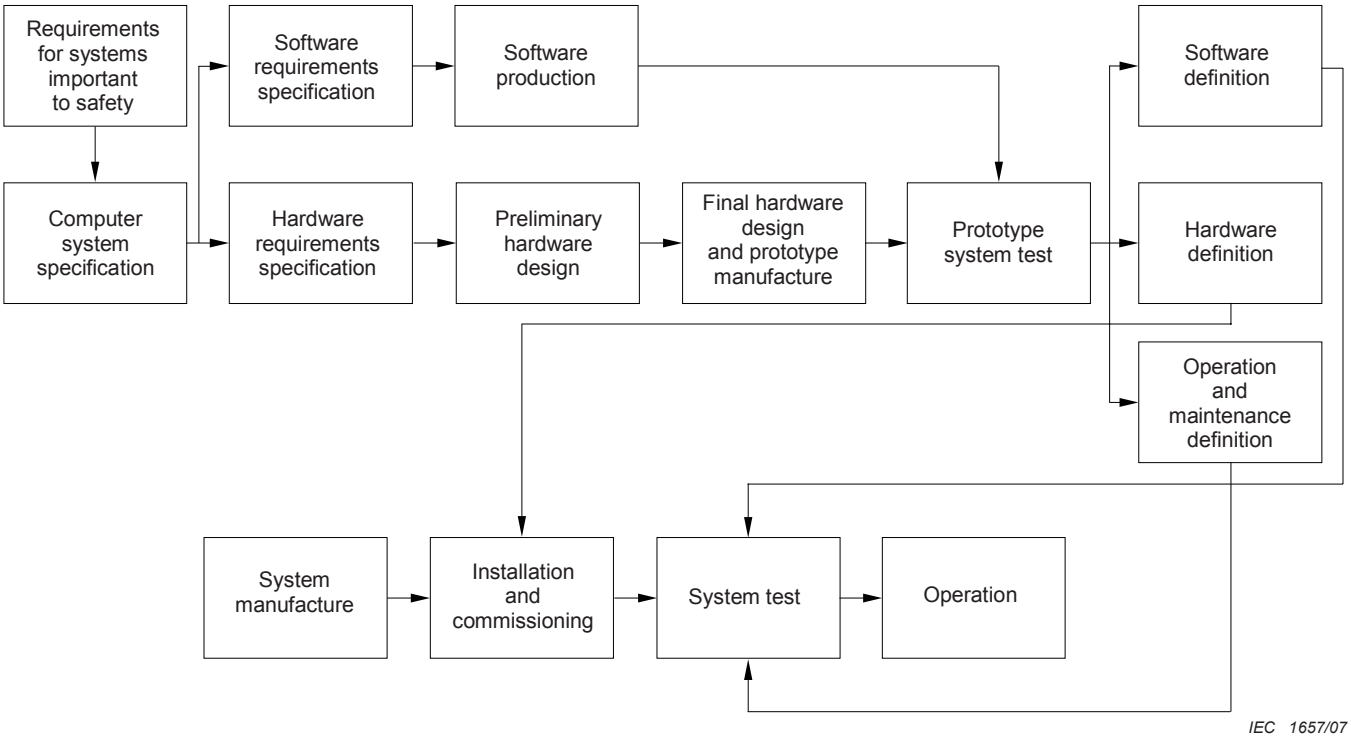
12.3 The design change procedure shall ensure that the impact of all hardware changes on the hardware and system verification, validation and qualification processes is identified and any required re-work is performed.

13 Operation

Relevant requirements for system operation are provided by IEC 61513 (IEC 60880 and IEC 62138 contain additional relevant information).

Annex A
(informative)

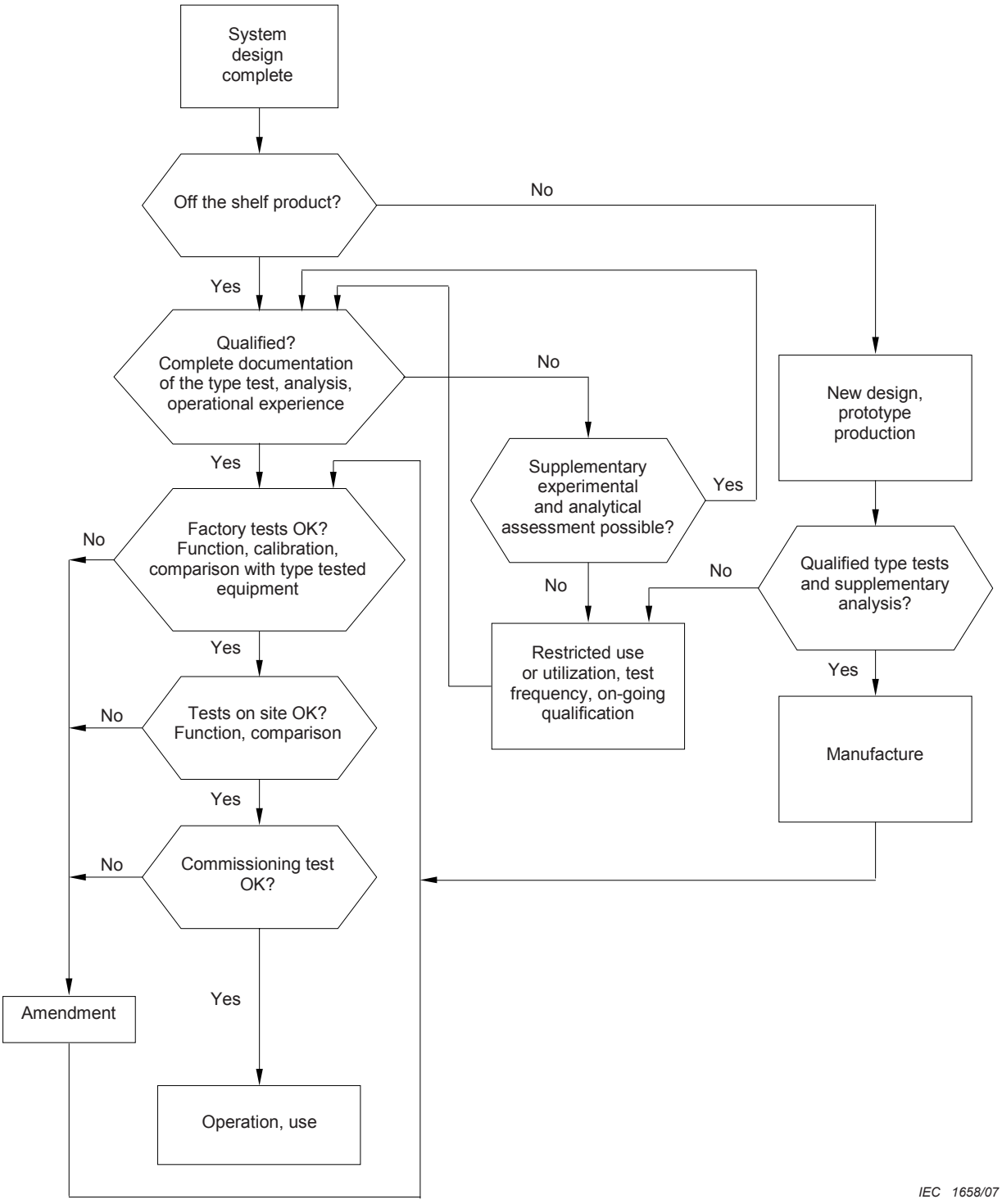
Overview of system life cycle



NOTE In the interest of clarity, the feedback paths have not been shown.

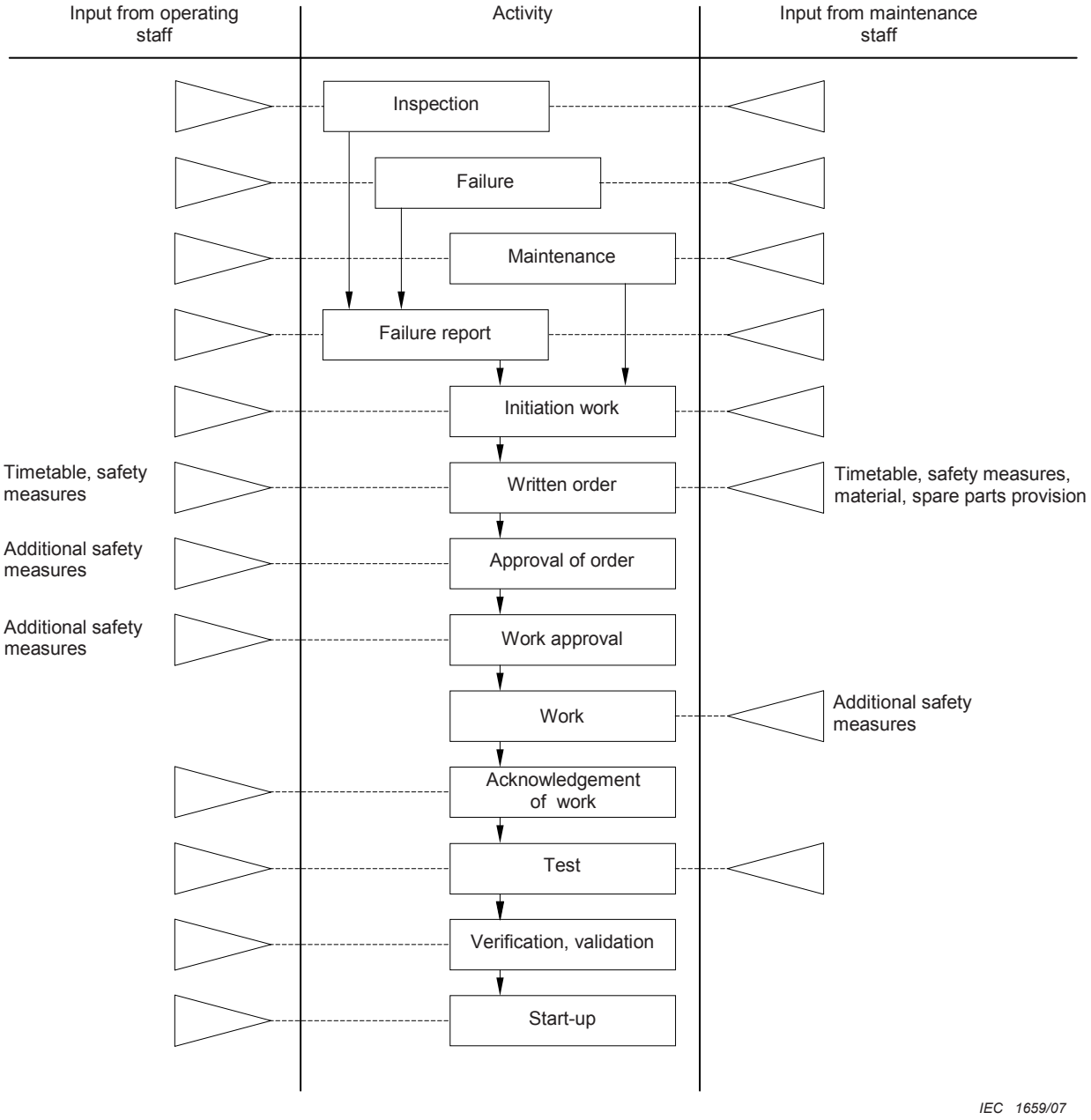
Annex B
(informative)

Outline of qualification

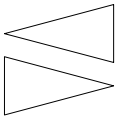


Annex C
(informative)

Example of maintenance procedure



Legend



Signifies staffing related to activity shown

Bibliography

The following references contain information of some relevance to this standard.

IEC 61226, *Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*

ISO 12207, *Information technology – Software life cycle process*

IAEA Safety Glossary:2006

IAEA NS-R-1:2000, *Safety of nuclear power plants: Design*

_____

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.

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 bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

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.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 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.

...making excellence a habit.™