

Nuclear instrumentation — A review of the application of IEC 60880 (1986)

ICS 27.120.20; 35.240.50

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This Published Document reproduces verbatim IEC 61940:1998.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation, which has the responsibility to:

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

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

From 1 January 1997, all IEC publications have the number 60000 added to the old number. For instance, IEC 27-1 has been renumbered as IEC 60027-1. For a period of time during the change over from one numbering system to the other, publications may contain identifiers from both systems.

Cross-references

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

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

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

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the CEI IEC title page, page ii, pages 1 to 17 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

Amendments issued since publication

Amd. No.	Date	Comments

This Published Document, having been prepared under the direction of the Engineering Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 January 1999

© BSI 05-1999

ISBN 0 580 32033 2

Contents

	Page
National foreword	Inside front cover
Text of CEI IEC 61940	1

**RAPPORT
TECHNIQUE
TECHNICAL
REPORT**

**CEI
IEC**

61940

Première édition
First edition
1998-06

**Instrumentation nucléaire –
Revue de l'application de la CEI 60880 (1986)**

**Nuclear instrumentation –
A review of the application of IEC 60880 (1986)**



Numéro de référence
Reference number
CEI/IEC 61940:1998

Contents

	Page
Introduction	1
1 Scope and object	1
2 Reference documents	1
3 Definitions and abbreviations	1
4 Assessment of compliance with IEC 60880	1
4.1 Purpose of assessment	1
4.2 Assessment process	1
5 Key assessment issues	2
5.1 Life cycle	2
5.2 Software types	4
5.3 Software changes	4
5.4 Reliability	5
5.5 Independence	5
6 Interpretation of specific clauses of IEC 60880	6

Introduction

IEC 60880 “Software for computers in the safety systems of nuclear power stations” was published in 1986. IEC 60880 (often referred to as the “Standard” in this report) has been widely used by system developers, to guide the development process, and by system assessors, who have used the standard to assess the fitness for purpose of systems.

This report provides an interpretation of IEC 60880, based upon feedback received from developers and assessors, which it is hoped will benefit future users of the Standard. Also, if IEC 60880 (1986) is revised at some later date, it is expected that the feedback of experience outlined in this report will be taken into account.

1 Scope and object

The purpose of this report is to combine the practical experience gained by users of IEC 60880 so as to provide an interpretation of IEC 60880 which will be of use to system developers and assessors. During the development of this report contributions have been received from many nations and the contents of this report is now believed to reflect the international experience regarding IEC 60880.

This report is not intended to represent an interpretation of IEC 60880 as applied on any specific project. It is written in a general manner and the suggested interpretations of IEC 60880 clauses should not be taken as definitive. This report does not replace, alter or add to the requirements contained in IEC 60880.

2 Reference documents

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*.

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*¹⁾.

ISO 9001:1994, *Quality systems — Model for quality assurance in design, development, production, installation and servicing*.

IAEA 50-SG-D3:1980, *Safety guide — Protection system and related features in nuclear power plants*.

3 Definitions and abbreviations

The definitions used in this technical report are given in clause 2 “Terms and definitions” of IEC 60880.

VDU: visual display unit

4 Assessment of compliance with IEC 60880

4.1 Purpose of assessment

There are many situations where an assessment against the Standard may be required, for example:

- a) during a system development process design engineers may assess the available methodologies and technologies against the Standard when deciding which would be the most appropriate to use;
- b) during the re-assessment of the safety case for an existing station the Standard may be used to assess the adequacy of operational systems;
- c) independent assessors may be required to confirm that a development process is compliant with the Standard.

The main purpose of assessing a system, or a system component, is to determine if it is demonstrably fit for use. If a system can be shown to essentially comply with IEC 60880 this provides some considerable confidence that it is suitable for use in a nuclear safety role.

4.2 Assessment process

Whether or not a particular system is considered to be “compliant” depends not only upon the characteristics of the system and its associated development life cycle, but also upon the skill of the assessor in interpreting the requirements and guidance provided by the Standard.

The Standard provides some guidance to assist in the interpretation of its contents, particularly the introduction which states that the Standard is to provide a “general approach” to software development, verification and validation; the Standard “discusses the software principles...” and provides “special recommendations” for safety systems. The use of such terminology implies that the contents of the Standard are not to be applied dogmatically, but that they should be used as guidance and should be interpreted as required for particular applications.

Clause 1, scope and object, also states that the appendices contain “Additional guidance and information on how to comply with the requirements of the main part of this Standard” — the emphasis is placed upon the contents of clause 3 to 10 rather than on those of Appendices A to F. The Standard requires that if techniques other than those identified in the appendices are used they are to be documented and auditable.

¹⁾ To be published.

Clauses in the main body of the Standard are qualified in a number of ways, for example “may”, “shall”, “required”, “should be”, “should be preferred”, “is recommended”. The significance of any deviations from the Standard depends upon the degree of compulsion implied by the text.

The end result of a formal assessment process should be a report identifying the particular clauses which are, in the opinion of the assessor, addressed or not addressed by a system. Documented justifications of compliance, in the form of explanations, references to manuals, reports, etc., should be provided for clauses for which compliance is claimed. Where the requirements/recommendations of a clause have not been followed, i.e. have not been complied with, the following classifications of response are suggested:

- a) not applicable, i.e. a coding recommendation not applicable to the language used, or a requirement outside the scope of the assessment, for example a requirement relevant to the purchaser/users of a system when performing an assessment of a system supplier, or a system requirement when the scope of an assessment is limited to assessment of the software production process;
- b) not yet applicable, for example if an assessment was performed before a system was delivered, all of the recommendations against system operation (clause 10 of IEC 60880) would fall into this category;
- c) not desirable, i.e. a recommendation which, for a particular application or development process, does not enhance safety/integrity;
- d) not compulsory, for example recommendations qualified with a “may”;
- e) minor non-compliance, i.e. a clear breach of the Standard but which has nil or minor impact upon the quality/safety of a system for example where an alternative and equivalent (or better) technique has been used to that recommended by the Standard;
- f) major non-compliance, i.e. a clear breach of the Standard which may have significant quality/safety implications.

Where non-compliance is identified a justification should be provided, to include a description of any mitigating factors.

It is suggested that, to improve clarity, the assessment report should contain a summary/conclusions section which considers the extent of overall compliance, including the identification of any aspects of the system which are “better” than that required by IEC 60880. A judgement should be given as to whether a system is fit for its proposed application and if the system is “generally” compliant with the Standard. Due to the broad scope of the Standard, and the need to interpret the Standard for an individual application, the determination of compliance is rarely a “black and white” issue and a qualified judgement may be required.

5 Key assessment issues

There are a number of key issues to be considered when assessing the compliance of a system.

5.1 Life cycle

The Standard defines a chronological progression from user requirements through to the final, integrated and tested system. Each phase is to be completed by a critical review (see comments on IEC 60880, subclause 3.1.6 in clause 6 of this report). In reality, and especially for large systems with a distributed processing architecture, there is usually a considerable degree of parallel working; the design process tends to be iterative in nature. Users will identify new requirements during the development process which have to be included in the design. No major non-compliance should be raised against the timing of various design activities providing that the fundamental principles of the Standard are addressed, namely that the final system is a manifestation of the users’ requirements and that the verification/validation processes are comprehensive, controlled and auditable.

Many of the requirements in the Standard implicitly assume a conventional top-down development life cycle for a bespoke system. Most “new” systems include components of old systems and to incorporate such components requires a degree of bottom-up design.

An example of a typical design process for a modern protection system is given below:

- a) the users develop a set of functional requirements;