
**Jedrske elektrarne - Merilna in nadzorna oprema za zagotavljanje varnosti -
Zahteve za obvladovanje odpovedi iz normalnih razlogov (CCF) (IEC 62340:2007)**

Nuclear power plants - Instrumentation and control systems important to safety -
Requirements for coping with Common Cause Failure (CCF) (IEC 62340:2007)

Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung -
Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC
62340:2007)

(standards.iteh.ai)

Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle
commande importants pour la sûreté - Exigences permettant de faire face aux
Défaillances de Cause Commune (DCC) (CEI 62340:2007)

Ta slovenski standard je istoveten z: EN 62340:2010

ICS:

27.120.20 Jedrske elektrarne. Varnost Nuclear power plants. Safety

SIST EN 62340:2010

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 62340:2010

<https://standards.iteh.ai/catalog/standards/sist/68395a2d-0c58-4217-a552-5f6d5886e96b/sist-en-62340-2010>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 62340

May 2010

ICS 27.120.20

English version

**Nuclear power plants -
Instrumentation and control systems important to safety -
Requirements for coping with Common Cause Failure (CCF)
(IEC 62340:2007)**

Centrales nucléaires de puissance -
Systèmes d'instrumentation et de contrôle
commande importants pour la sûreté -
Exigences permettant de faire face
aux Défaillances de Cause Commune
(DCC)
(CEI 62340:2007)

Kernkraftwerke -
Leittechnische Systeme
mit sicherheitstechnischer Bedeutung -
Anforderungen zur Beherrschung
von Versagen aufgrund gemeinsamer
Ursache
(IEC 62340:2007)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This European Standard was approved by CENELEC on 2010-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of the International Standard IEC 62340:2007, prepared by SC 45A, Instrumentation and control of nuclear facilities, of IEC TC 45, Nuclear instrumentation, was submitted to the CENELEC formal vote for acceptance as a European Standard and was approved by CENELEC as EN 62340 on 2010-05-01.

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

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2011-05-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2013-05-01

Annex ZA has been added by CENELEC.

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 European Standard.”

SIST EN 62340:2010

[https://standards.iteh.ai/catalog/standards/sist/68395a2d-0c58-4217-a552-](https://standards.iteh.ai/catalog/standards/sist/68395a2d-0c58-4217-a552-5f6d5886e96b/sist-en-62340-2010)

[5f6d5886e96b/sist-en-62340-2010](https://standards.iteh.ai/catalog/standards/sist/68395a2d-0c58-4217-a552-5f6d5886e96b/sist-en-62340-2010)

Endorsement notice

The text of the International Standard IEC 62340:2007 was approved by CENELEC as a European Standard without any modification.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

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

| <u>Publication</u> | <u>Year</u> | <u>Title</u> | <u>EN/HD</u> | <u>Year</u> |
|----------------------------|-------------|--|--------------|-------------|
| IEC 60671 | - | Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing | - | - |
| IEC 60709 | - | Nuclear power plants - Instrumentation and control systems important to safety - Separation | EN 60709 | - |
| IEC 60780 | - | Nuclear power plants - Electrical equipment of the safety system - Qualification | - | - |
| 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 60980 | - | Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations | - | - |
| IEC 61000-4 | Series | Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques | EN 61000-4 | Series |
| IEC 61226 | - | Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions | - | - |
| IEC 61513 | - | Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems | - | - |
| IAEA Safety Guide NS-G-1.3 | - | Instrumentation and control systems important to safety in nuclear power plants | - | - |
| IAEA Safety Guide SG-D11 | - | General design safety principles for nuclear power plants; a safety guide | - | - |
| IAEA Safety Glossary | 2007 | Terminology used in nuclear safety and radiation protection | - | - |

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 62340:2010

<https://standards.iteh.ai/catalog/standards/sist/68395a2d-0c58-4217-a552-5f6d5886e96b/sist-en-62340-2010>



IEC 62340

Edition 1.0 2007-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Nuclear power plants – Instrumentation and control systems important to safety
– Requirements for coping with common cause failure (CCF)**

**Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-
commande importants pour la sûreté – Exigences permettant de faire face aux
défaillances de cause commune (DCC)**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

T

CONTENTS

| | |
|--|----|
| FOREWORD..... | 3 |
| INTRODUCTION..... | 5 |
| 1 Scope..... | 7 |
| 2 Normative references | 8 |
| 3 Terms and definitions | 8 |
| 4 Abbreviations | 12 |
| 5 Conditions and strategy to cope with CCF | 13 |
| 5.1 General..... | 13 |
| 5.2 Characteristics of CCF | 13 |
| 5.3 Principal mechanisms for CCF of digital I&C systems..... | 13 |
| 5.4 Conditions to defend against CCF of individual I&C systems | 14 |
| 5.5 Design strategy to overcome CCF | 15 |
| 6 Requirements to overcome faults in the requirements specification | 15 |
| 6.1 Deriving the requirements specification for the I&C from the plant safety design base..... | 15 |
| 6.2 Application of the defence-in-depth principle and functional diversity | 16 |
| 6.3 CCF related issues at existing plants..... | 17 |
| 7 Design measures to prevent coincidental failure of I&C systems..... | 17 |
| 7.1 The principle of independence..... | 17 |
| 7.2 Design of independent I&C systems | 18 |
| 7.3 Application of functional diversity..... | 18 |
| 7.4 Avoidance of failure propagation via communications paths | 19 |
| 7.5 Design measures against system failure due to maintenance activities..... | 19 |
| 7.6 Integrity of I&C system hardware..... | 19 |
| 7.7 Precaution against dependencies from external dates or messages | 20 |
| 7.8 Assurance of physical separation and environmental robustness..... | 20 |
| 8 Tolerance against postulated latent software faults | 20 |
| 9 Requirements to avoid system failure due to maintenance during operation | 21 |
| Annex A (informative) Relation between IEC 60880 and this standard | 22 |

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
INSTRUMENTATION AND CONTROL
SYSTEMS IMPORTANT TO SAFETY –
REQUIREMENTS FOR COPING WITH
COMMON CAUSE FAILURE (CCF)**

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 62340 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

| | |
|--------------|------------------|
| FDIS | Report on voting |
| 45A/668/FDIS | 45A/676/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.

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

SIST EN 62340:2010

<https://standards.iteh.ai/catalog/standards/sist/68395a2d-0c58-4217-a552-5f6d5886e96b/sist-en-62340-2010>

INTRODUCTION

a) Background, main issues and organisation of this Standard

In order to achieve a high safety level, redundancy is applied as one of the key features for designing instrumentation and control systems (I&C systems) important to safety. Since a Common Cause Failure (CCF) could compromise the effectiveness of redundancy, it is essential to take adequate measures against it. The nuclear industry has pioneered systems design and engineering to address CCF. Over the last thirty years it has implemented and reached consensus on a number of practices to handle and overcome CCF.

The intention of this standard is to address the whole scope of aspects to overcome Common Cause Failures (CCFs) and to provide an overview of the relevant requirements for I&C systems that are used to perform functions important to safety (according to IEC 61226) in nuclear power plants.

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

IEC 62340 is a second level IEC SC 45A document tackling the issue of CCF.

This international standard supplements IEC 61513 and related standards with requirements to reduce and overcome the possibility of CCF of I&C functions of category A. The requirements given by this standard are applicable to category A (IEC 61226) functions if their failure would be unacceptable with respect to the plant safety design.

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

c) Recommendations and limitations regarding the application of this Standard

This standard applies to I&C systems important to safety of new NPPs as well as to the replacement of I&C systems of existing plants. The I&C functions may need to be kept or upgraded if an I&C system is replaced. The requirements of this standard also consider the replacement of I&C which entails changes in the structure of I&C systems.

For existing plants, only a subset of the requirements from this standard may be applicable and this subset should be identified at the beginning of any project. The requirements and recommendations which are not to be implemented in an I&C upgrading or replacement project should be justified on a case by case basis by an overall safety assessment. The potential consequences of not following this standard in some aspects due to plant constraints should be considered in comparison to the added safety gained through the upgrade as a whole.

To avoid overlapping requirements, this standard takes advantage of other existing standards by referring to the relevant (sub)clauses, especially to the nuclear sector standards IEC 61513, IEC 60709, IEC 60780 and IEC 60880. New requirements are given where not covered by these standards.

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

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 directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems,