



SLOVENSKI STANDARD SIST EN IEC 62859:2020

01-november-2020

Jedrske elektrarne - Merilna in nadzorna oprema - Zahteve za usklajevanje varnosti in kibernetike varnosti (IEC 62859:2016+A1:2019)

Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity (IEC 62859:2016+A1:2019)

Kernkraftwerke - Leittechnische Systeme - Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit (IEC 62859:2016+A1:2019)

Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle-commande - Exigences pour coordonner sûreté et cybersécurité (IEC 62859:2016+A1:2019)

<https://standards.iteh.ai/catalog/standards/sist/257dcd44-2701-47d8-8fe0-8a3ae14e190c/sist-en-iec-62859-2020>

Ta slovenski standard je istoveten z: EN IEC 62859:2020

ICS:

27.120.20 Jedrske elektrarne. Varnost Nuclear power plants. Safety

SIST EN IEC 62859:2020

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN IEC 62859:2020

<https://standards.iteh.ai/catalog/standards/sist/257dcd44-2701-47d8-8fe0-8a3ae14e190c/sist-en-iec-62859-2020>

EUROPEAN STANDARD

EN IEC 62859

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2020

ICS 27.120.20

English Version

Nuclear power plants - Instrumentation and control systems -
Requirements for coordinating safety and cybersecurity
(IEC 62859:2016 + A1:2019)

Centrales nucléaires de puissance - Systèmes
d'instrumentation et de contrôle-commande - Exigences
pour coordonner sûreté et cybersécurité
(IEC 62859:2016 + A1:2019)

Kernkraftwerke - Leittechnische Systeme - Anforderungen
für die Koordinierung von Sicherheit und IT-Sicherheit
(IEC 62859:2016 + A1:2019)

This European Standard was approved by CENELEC on 2020-07-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

SIST EN IEC 62859:2020

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, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

EN IEC 62859:2020 (E)**European foreword**

The text of document 45A/1104/FDIS, future IEC 62859/A1, prepared by SC 45A "Instrumentation, control and electrical power systems of nuclear facilities" of IEC/TC 45 "Nuclear instrumentation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62859:2020.

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) 2021-07-20
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-07-20

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

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 and/or security measures in the subject-matter covered by this standard.

SIST EN IEC 62859:2020
<https://standards.iteh.ai/catalog/standards/sist/257dcd44-2701-47d8-8fe0-8a3ae14c1969/sist-en-iec-62859-2020>
Endorsement notice

The text of the International Standard IEC 62859:2016/A1:2019 was approved by CENELEC as a European Standard without any modification.

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

IEC 61508-1	NOTE	Harmonized as EN 61508-1
IEC 61508-2	NOTE	Harmonized as EN 61508-2
IEC 61508-3	NOTE	Harmonized as EN 61508-3
IEC 61508-4	NOTE	Harmonized as EN 61508-4

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 1 Where 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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60709	2004	Nuclear power plants - Instrumentation and control systems important to safety - Separation	EN 60709	2010
IEC 60880	2006	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	EN 60880	2009
IEC 61500	2009	Nuclear power plants - Instrumentation and control important to safety - Data communication in systems performing category A functions	EN 61500	2011
IEC 61513	2011	Nuclear power plants - Instrumentation and control important to safety - General requirements for systems	EN 61513	2013
IEC 62138	2004	Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions	EN 62138	2009
IEC 62340	-	Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)	EN 62340	-
IEC 62566	2012	Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions	EN 62566	2014
IEC 62646	2016	Nuclear power plants - Control rooms - Computer-based procedures	EN IEC 62646	2019

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN IEC 62859:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/257dcd44-2701-47d8-8fe0-8a3ae14e190c/sist-en-iec-62859-2020>



IEC 62859

Edition 1.0 2016-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences pour coordonner sûreté et cybersécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-3719-9

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 Symbols and abbreviations.....	11
5 Coordinating safety and cybersecurity at the overall architecture level	12
5.1 General.....	12
5.2 Fundamental and generic principles.....	12
5.3 Thematic requirements and recommendations	13
5.3.1 Delineation of security zones	13
5.3.2 Provisions for coping with common cause failures (including diversity)	13
5.3.3 Separation provisions	14
5.3.4 Data communications	14
6 Coordinating safety and cybersecurity at the individual system level.....	14
6.1 General.....	14
6.2 Fundamental and generic principles.....	14
6.3 Safety and cybersecurity coordination during the I&C system lifecycle	15
6.3.1 General	15
6.3.2 Requirements and planning activities.....	15
6.3.3 Design activities	15
6.3.4 Implementation activities	16
6.3.5 Verification and validation activities	16
6.3.6 Installation and acceptance testing activities	16
6.3.7 Operations and maintenance activities.....	16
6.3.8 Change management.....	16
6.3.9 Decommissioning activities.....	16
6.4 Selected technical aspects of I&C systems constrained by safety and cybersecurity	17
6.4.1 General	17
6.4.2 Logical access control for HMIs of I&C programmable digital systems in control rooms.....	17
6.4.3 Software modification	17
6.4.4 Logging and audit capability	18
6.4.5 Use of cryptography by I&C systems	18
6.4.6 System availability and function continuity.....	19
7 Organizational and operational issues	19
7.1 Governance and responsibilities	19
7.2 Coordination between safety and cybersecurity staff during operations.....	19
7.3 Safety and cybersecurity culture	19
7.4 Emergency response management	19
Annex A (informative) Rationale for, and notes related to, the scope of this document.....	21
A.1 General.....	21
A.2 Inclusion of I&C programmable digital system not important to safety	21
A.3 Exclusion of physical security, room access control and site security surveillance systems.....	21

A.4	Exclusion of non-malevolent actions and events	21
A.5	Exclusion of development tools and platforms.....	22
	Bibliography.....	23

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN IEC 62859:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/257dcd44-2701-47d8-8fe0-8a3ae14e190c/sist-en-iec-62859-2020>

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
INSTRUMENTATION AND CONTROL SYSTEMS –
REQUIREMENTS FOR COORDINATING SAFETY AND CYBERSECURITY**

FOREWORD

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

International Standard IEC 62859 has been prepared by subcommittee 45A: Instrumentation, control and electrical systems 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/1104/FDIS	45A/1118/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 stability date indicated on the IEC website 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 IEC 62859:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/257dcd44-2701-47d8-8fe0-8a3ae14e190c/sist-en-iec-62859-2020>

INTRODUCTION

a) Technical background, main issues and organisation of this standard

I&C systems have evolved during the last decades from non-digital equipment and stand-alone environments to digital technologies and interconnected systems. Such an evolution exposes them to risks related to cyberattacks. In addition to well-established safety-oriented provisions, more recent cybersecurity requirements and controls now apply to the same systems. A normative framework is needed to master the interactions and potential side-effects when safety and cybersecurity provisions converge on the same I&C systems and architectures, taking into account the nuclear I&C specifics and the SC 45A related standards.

This standard specifically focuses on the issue of requirements for coordinating safety and cybersecurity provisions for I&C programmable digital systems and architectures. It defines both generic principles and guidance for practical situations to integrate cybersecurity requirements in nuclear I&C architectures and systems, fundamentally tailored for safety. Technical but also conceptual, organizational and procedural aspects are covered.

It is intended that this standard be used by designers and operators of nuclear power plants (NPPs) (utilities), systems evaluators, vendors and subcontractors, and by licensors.

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

IEC 62859 is at the second level of the IEC SC 45A standard series. It is to be considered as bridging IEC 62645 (also at the second level of the IEC SC 45A standard series) and IEC 61513, the top level document of the IEC SC 45A standard series. Regarding the specific theme of cybersecurity, IEC 62645 is the top-level in the SC 45A standard series. Both IEC 62645 and IEC 62859 are considered formally as second level documents with respect to IEC 61513, although IEC 61513:2011 does not actually ensure proper reference to and consistency with them (this will be done in a future revision of IEC 61513).

For a generic description of 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

It is important to note that this standard establishes additional requirements for I&C programmable digital systems and architectures, with regard to the coordination between safety and cybersecurity, and clarifies the processes by which I&C programmable digital systems are designed, implemented and operated in nuclear power plants. Aspects for which special requirements and recommendations have been produced are:

- IAEA guidance on I&C;
- IAEA guidance on computer security at nuclear facilities;
- regulatory interpretations for country specific requirements.

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 documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046¹. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply

¹ In preparation. Stage at the time of publication: IEC ANW 63046:2016.