IEC 62859

Edition 1.1 2019-10

FINAL VERSION

VERSION FINALE

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

IEC 62859:2016-10+AMD1:2019-10 CSV(en-fr)

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

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.

DISCLAIMER
This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62859 bears the edition number 1.1. It consists of the first edition (2016-10) [documents 45A/1104/FDIS and 45A/1118/RVD] and its amendment 1 (2019-10) [documents 45A/1279/FDIS and 45A/1286/RVD]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

© IEC 2019

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.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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 63046[1]. 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.

systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPP), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPP, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPP, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPP and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 will be published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

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

1 Scope

This document provides a framework to manage the interactions between safety and cybersecurity for nuclear power plant (NPP) systems, taking into account the current SC 45A standards addressing these issues and the specifics of nuclear I&C programmable digital systems.

NOTE In this document (as in IEC 62645), cybersecurity relates to prevention of, detection of, and reaction to malicious acts perpetrated by digital means (cyberattacks). In this context, it does not cover considerations related to non-malevolent actions and events such as accidental failures, natural events or human errors (except those degrading cybersecurity). Those aspects are of course of prime importance but they are covered by other SC 45A documents and standards, and are not considered as cybersecurity related in this document.

This document establishes requirements and guidance to:

– integrate cybersecurity provisions in nuclear I&C architectures and systems, which are fundamentally tailored for safety;
– avoid potential conflicts between safety and cybersecurity provisions;
– aid the identification and the leveraging of the potential synergies between safety and cybersecurity.

This document is intended to be used for designing new NPPs, or modernizing existing NPPs, throughout I&C programmable digital systems lifecycle. It is also applicable for assessing the coordination between safety and cybersecurity of existing plants. It may also be applicable to other types of nuclear facilities.

This document addresses I&C programmable digital systems important to safety and I&C programmable digital systems not important to safety. It does not address programmable digital systems dedicated to site physical security, room access control and site security surveillance.

This document is limited to I&C programmable digital systems of NPPs, including their on-site maintenance and configuration tools.

Annex A provides a rationale for and comments about the scope definition and the document application, in particular about the exclusions and limitations previously mentioned.

This document comprises three normative clauses:

- Clause 5 deals with the overall I&C architecture;
- Clause 6 focuses on the system level;
- Clause 7 deals with organizational and operational issues.

2 Normative references

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.