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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

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

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.

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.

IEC 60709:2004, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61500:2009, *Nuclear power plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IEC 62645:2014, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62645, in IEC 61513 and the following apply.

NOTE If for a given term, different definitions are provided in these three sources, the definition of the present document applies.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
computer-based item
item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: A computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to software-based item.

3.2
cyberattack
attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Note 1 to entry: Cyberattacks include targeted and non-targeted (e.g. malwares) attacks by digital means. Cyberattack is synonymous with digital attack.

3.3
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

- malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation;
- malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;
- malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

Note 1 to entry: This definition is tailored with respect to this standard scope and overall SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the SC 45A standard series. See Annex A.4 for more detail about such exclusions.

Note 2 to entry: Computer security, security and cybersecurity are considered synonymous in this document.

3.4
cybersecurity event
identified occurrence of a system, service or network state indicating a possible breach of cybersecurity policy or failure of controls, or a previously unknown situation that may be cybersecurity relevant

3.5
cybersecurity-driven software modification
software modification of which the main reason is to implement one or more cybersecurity features, or remediate one or several security vulnerabilities in a I&C programmable digital component, or to prevent successful exploitation of these vulnerabilities or to mitigate attackers’ capabilities to exploit these vulnerabilities

3.6
cybersecurity feature
provision, control or function specifically designed for cybersecurity purposes

Note 1 to entry: Non-cybersecurity features implementation can have negative, neutral, but also positive impact on cybersecurity. This is particularly the case of some safety features, as discussed in this document.

Note 2 to entry: The terms “feature” and “provision” are considered synonymous in this document.

3.7
HDL-Programmed Device
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools

Note 1 to entry: HDLs and related tools (e.g. simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2 to entry: The development of HPDs can use pre-developed blocks.

Note 3 to entry: HPDs are typically based on blank FPGAs (Field Programmable gate Arrays) or similar programmable integrated circuits.

[SOURCE: IEC 62566:2012, 3.7]

3.8
logical separation
separation from a digital data network perspective involving the absence of direct data communications (i.e. without any proxy or cybersecurity filtering device)

3.9
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: The main programmable digital items are computer-based items and programmable logic items.

Note 3 to entry: This term used by SC 45A is equivalent to Programmable Electronic item used in IEC 61508.

3.10
programmable logic item
item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: A programmable logic item is a kind of programmable digital item.

3.11
safety feature
provision, control or function specifically designed for safety purposes

Note 1 to entry: Non-safety features implementation can have negative, neutral, but also positive impact on safety. This is particularly the case of some cybersecurity features, as discussed in this standard.

Note 2 to entry: The terms "feature" and "provision" are considered synonymous.

3.12
software modification
change in an already agreed document (or documents) leading to an alteration of the executable code

Note 1 to entry: Software modifications may occur either during initial software development (e.g. to remove faults found in later stages of development), or after the software is already in service.

[SOURCE: IEC 60880:2006, 3.36]

3.13
software security update
piece of software provided by a digital system supplier and designed to fix one or several security vulnerabilities in a digital component, or implement one or more cybersecurity features

Note 1 to entry: Security patches are considered as software security updates.

4 Symbols and abbreviations

BIOS	Basic Input/Output System
CB	Computer-Based
CCF	Common Cause Failure
CRC	Cyclic Redundancy Check
FPGA	Field-Programmable Gate Array
HDL	Hardware Description Language
HMI	Human-Machine Interface

HPD	HDL-Programmed Device
I&C	Instrumentation and Control
NPP	Nuclear Power Plant

5 Coordinating safety and cybersecurity at the overall architecture level

5.1 General

Several safety features and architectural characteristics implemented in order to address design basis requirements are in some cases directly beneficial to cybersecurity: this includes some of the features that support equipment independence, system reliability or system diversity. However, considering that the design of these features may not have adequately taken into account potential vulnerabilities to cyberattacks, dedicated cybersecurity measures may be needed to achieve adequate cybersecurity, without degrading safety.

This clause provides requirements and recommendations to enable a smooth integration of cybersecurity requirements as per IEC 62645 in a nuclear I&C architecture, fundamentally and firstly structured by safety-oriented requirements (in particular those of IEC 61513 and several second level documents of the SC 45A series, including IEC 62340 or IEC 60709).

5.2 Fundamental and generic principles

The following principles apply for the treatment of cybersecurity at the I&C architectural level:

a) Cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realisation. It shall not compromise the effectiveness of the diversity and defence-in-depth features implemented by the I&C architecture.

b) Cybersecurity requirements impacting the overall I&C architecture shall be addressed after the overall I&C architecture design and assignment of the I&C functions have been first made as per 5.4 of IEC 61513:2011. The integration of architectural cybersecurity requirements may lead to an iterative design process.

NOTE The objective is to secure a safe I&C architecture. Such a sequence is already implicit in IEC 62645, as the assignment of security degrees (and their associated requirements) assumes that safety categories are already assigned to safety functions, and that the safety functions are already assigned to I&C systems.

c) Cybersecurity features shall not adversely impact the required performance (including response time), required effectiveness, required reliability or required operation of functions important to safety.

d) The failure modes and consequences of cybersecurity features on the functions important to safety shall be analysed and taken into account.

e) When two architecture designs offer equivalent level of safety, priority should be given to the most secure one. Unnecessary complexity shall be avoided as it is detrimental to both safety and cybersecurity.

f) Any architectural property or characteristics designed for safety reason (e.g., independence between systems), which has value as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined taking into account context-relevant cyberattacks, by staff responsible for cybersecurity, to confirm its cybersecurity effectiveness.

A particular case corresponds to communications between systems important to safety and systems not important to safety, or between systems of different safety classes. IEC 61513 already requires that communication links are designed in such a way that data communication and operation of the higher safety category function cannot be jeopardised by data communication with lower classified systems. However, the provisions taken to fulfil such safety requirements are not necessarily robust against malicious threats and cyberattacks.

5.3 Thematic requirements and recommendations

5.3.1 Delineation of security zones

5.3.1.1 General

As defined in IEC 62645, security zones are practical and architectural implementations of a graded approach to cybersecurity; they allow I&C systems with similar importance concerning safety and plant performance (i.e. having the same security degree) to be grouped together for administration and application of protective measures. As per IEC 62645, criteria for defining a security zone include organizational issues (such as ownership/responsibility), localisation, architectural or technical aspects. In practice, security zones are implemented as means against the propagation of cyberattacks. In such context, when a zone model is enforced as recommended by IEC 62645, the following applies:

a) The delineation of security zones, as per IEC 62645, shall take into account and leverage independence and physical separation requirements introduced for the purpose of enhancing safety.

b) Data communication aspects (incl. logical separation) and geographical/physical separation as well as independence aspects shall be considered together to delineate security zones.

NOTE Geographical separation and independence features are not sufficient to delineate security zones.

5.3.1.2 Dealing with systems with several divisions

a) The divisions (or trains) of a given I&C programmable digital system should be grouped in the same security zone, unless the communications between divisions can be efficiently filtered and monitored from a cybersecurity perspective.

b) The divisions (or trains) of a given I&C programmable digital system shall be grouped in the same security zone if a common engineering tool is used to configure them.

NOTE This requirement holds even if the tool is connected only to one division at a time: if the tool is compromised, it can support an asynchronous attack, compromising divisions one after the other.

5.3.1.3 Dealing with systems sharing common resources

a) I&C programmable digital systems sharing common computer-based tools (e.g. configuration, testing, and/or maintenance tools) shall be grouped in the same security zone, unless it is demonstrated from a cybersecurity perspective that the tools cannot directly impact the systems they are connected to.

b) I&C programmable digital systems sharing a common network or communication bus without cybersecurity technical provisions securing the communications should be grouped in the same security zone, even if they perform functions of different safety categories. As per IEC 62645, the security degree assignment shall take into account the most sensitive safety category.

5.3.2 Provisions for coping with common cause failures (including diversity)

a) In some cases, provisions taken in order to cope with common cause failures (CCF), including diversity, can be leveraged from a cybersecurity perspective, and should be leveraged in such cases. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and potential cyberattacks (consistently with 5.2 f).

NOTE 1 Provisions resulting from requirements, recommendations and associated safety practices as per 5.4.2.6 of IEC 61513:2011 (for all I&C systems important to safety), Clause 13 of IEC 60880:2006 (for software aspects of systems performing category A functions), IEC 62340 or equivalent (for systems performing category A functions), are for instance directly concerned by 5.3.2a).

NOTE 2 As for safety, diversity is also commonly used in cybersecurity: examples include the use of diverse penetration testing tools, diverse skills of cybersecurity team members or auditors. However, expecting benefit from diversity in all situations for both safety and cybersecurity is questionable. Diversity is generally used "in series" to bring cybersecurity benefit (involving the need to compromise one system after another to reach a target), whereas it is generally used "in parallel" to bring benefit in safety. Such use "in parallel" is in some