BS IEC 62859:2016

BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of IEC 62859:2016.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Instrumentation, Control & Electrical Systems of Nuclear Facilities.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 86459 9
ICS 27.120.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2016.

Amendments/corrigenda issued since publication

Date	Text affected

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

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

cases antagonistic with cybersecurity, increasing the attack surface. Moreover, even from a pure cybersecurity perspective there are pros and cons to diversity. Used "in series" (for instance two firewalls from different providers), diversity makes the attacker task more complex (avoiding common vulnerabilities, cybersecurity functions completing each others), but at the same time, it introduces complexity leading to higher risk of configuration errors, difficulty of maintenance, etc.

b) Any cybersecurity measures considered for inclusion in the design shall be assessed for their potential to introduce fault leading to CCF between systems diversified for safety reasons. Where such risks are found, alternative means of achieving adequate cybersecurity shall be implemented as necessary.

5.3.3 Separation provisions

a) In some cases, provisions taken for separation purposes can be leveraged from a cybersecurity perspective, and should be leveraged in such cases.

b) Requirements, recommendations and associated safety practices as per 5.4 of IEC 60709:2004 on independence from control systems (for systems supporting category A functions), or equivalent, are potentially beneficial both in terms of safety and cybersecurity. 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).

5.3.4 Data communications

a) Requirements, recommendations and associated safety practices as per IEC 61500:2009 on data communications (for systems supporting category A functions), or equivalent, are potentially beneficial both in terms of safety and cybersecurity. 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 cyberattacks (consistently with 5.2 f).

b) A detailed knowledge of data communications in use by and between I&C programmable digital systems (incl. protocols, roles, initiatives, sources and destinations) is beneficial both for safety and cybersecurity and shall be maintained and documented, from design to implementation and operations.

6 Coordinating safety and cybersecurity at the individual system level

6.1 General

In addition to the architectural level treated in Clause 5, coordination of safety and cybersecurity shall also be considered at the individual system level. This clause provides requirements and recommendations for such coordination.

6.2 Fundamental and generic principles

The following principles apply for the treatment of cybersecurity features on I&C programmable digital systems:

a) Implementation of cybersecurity features directly in systems important to safety shall be justified.

NOTE 1 Adding cybersecurity features to system important to safety increases system complexity and has the potential to introduce new failure modes to the system. Such consequences can challenge the system ability to perform its function(s) important to safety in a reliable manner. Moreover, the rapid evolution pace of cybersecurity threats, vulnerabilities and techniques is hard to conciliate with the modification processes of systems important to safety. However, a limited number of cybersecurity controls are still in some cases implemented in systems important to safety: examples include logging capability and authentication mechanisms, as per 5.5.3 of IEC 61513:2011 and as per IEC 62645.

NOTE 2 Implementation of cybersecurity features outside systems important to safety ease separate qualification of cybersecurity related features when required by national regulations.

b) Cybersecurity features shall not adversely impact the realisation of functions important to safety, the required performance (including response time), required reliability, or required operation of programmable digital systems important to safety.

NOTE 3 Key elements of I&C programmable digital system performance are for example task ordering, functional parameters, maximum response time of functions and maximum usage of resources. Cybersecurity features implementation is likely to influence, even marginally, one or several of these elements: the important criterion is that it does not prevent the system from meeting the required performance to ensure its functions.

c) The failure modes and consequences of these cybersecurity features on the system's functions important to safety shall be analysed and taken into account.

d) Cybersecurity features implemented in systems important to safety shall be developed and qualified to the same level as the system these features reside in.

e) If cybersecurity features are implemented in displays and controls of systems important to safety, they shall not adversely impact the operator's ability to maintain plant safety.

f) When a cybersecurity requirement cannot be met by the implementation of a cybersecurity feature in a system important to safety, alternative cybersecurity measures shall be implemented. These alternative measures shall at least ensure that the system's security degree requirements (as per IEC 62645) are met.

NOTE 4 Such alternative measures can be for instance organisational, architectural, or in particular dealing with the communications and interfaces with the system.

g) Safety-oriented procedures (e.g. surveillance tests) or functions have been implemented to fulfil safety objectives. When reusing a safety procedure or function to achieve cybersecurity objectives, both the safety objectives and the cybersecurity objectives of the reused procedure or function shall be described, and their achievement shall be justified and documented.

h) The extension or modification of a safety-oriented procedure (e.g., surveillance tests) or function for cybersecurity purpose can only be made if it has been previously justified and documented that its safety objectives are still achieved.

6.3 Safety and cybersecurity coordination during the I&C system lifecycle

6.3.1 General

The requirements and recommendations provided in 6.2 do not specifically consider the lifecycle phases of I&C programmable digital systems. The objective of 6.3 is to provide additional requirements and considerations with respect to I&C programmable digital system lifecycle activities. For consistency reasons, the activities considered are those used in Clause 6 of IEC 62645:2014.

NOTE The order of Subclauses 6.3.2 to 6.3.9, adopted from IEC 62645:2014, does not necessarily present the timely order of activities which are sometimes in reality partially executed in parallel, or include iterations.

6.3.2 Requirements and planning activities

a) Cybersecurity requirements should be defined as early as possible in the I&C programmable digital system lifecycle.

b) Potential dependencies, conflicts or reinforcements between safety requirements and cybersecurity requirements should be detected, documented and taken into account to ensure the definition of an integrated solution meeting both the safety and security goals.

6.3.3 Design activities

a) I&C systems should be designed in order to favour reinforcements between safety and cybersecurity features. Related design choices regarding such reinforcements should take into account a trade-off analysis between:

   – the gains and drawbacks related to the verification and validation of the systems;

   – the gains and drawbacks in terms of system complexity and interfaces.

b) Any system feature initially designed for safety reason which has a potential value as a 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.

c) The security features of programmable digital systems important to safety should be designed to limit their dependency on updates.

6.3.4 Implementation activities

This document does not provide any specific requirements or recommendations related to the coordination between safety and cybersecurity for this phase. Refer to IEC 62645 for cybersecurity-related ones, to IEC 60880 and IEC 62138 for software of CB I&C systems supporting functions important to safety, and to IEC 62566 for HDL-programmed integrated circuits for systems performing category A functions.

6.3.5 Verification and validation activities

a) Software code review or analysis of I&C programmable digital systems conducted for safety reasons (see IEC 60880 and IEC 62138 for software of systems performing functions important to safety) may also consider cybersecurity aspects and vulnerabilities associated with unsecure coding practices.

NOTE 1 Skills and tools needed for safety-oriented code review or analysis, and those needed for security-oriented code review or analysis are often overlapping, however, they are different. The optimal level of integration of these activities is highly dependent on the context.

b) Appropriate cybersecurity measures should be taken to protect sensitive data or information associated to software code review and analysis.

c) Software and hardware should be verified and validated in order to avoid unapproved functionalities. This may be required from a safety perspective (as per the applicable standards), but also from a cybersecurity perspective in some cases.

NOTE 2 During inspections made for hardware verification and validation, wireless capabilities or undeclared programmable digital components can be detected.

6.3.6 Installation and acceptance testing activities

a) Security tests should be conducted in a test environment representative of the installed system.

6.3.7 Operations and maintenance activities

a) Off-line maintenance periods should be considered as opportunities for software security updates, if compatible with respect to qualification constraints.

b) Periodic testing of functions important to safety shall not degrade cybersecurity of the involved I&C systems.

c) Cybersecurity verifications may be considered for integration in safety periodic testing.

NOTE Such integrations are subject to restrictions: see 6.2 g) and 6.2 h).

d) Intrusive security testing, including penetration testing, shall not be conducted directly on systems important to safety during operations. A test lab should be available.

6.3.8 Change management

a) There shall be procedures to assess and manage the potential for adverse safety and cybersecurity interactions that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures.

b) There should be procedures to identify and leverage potential mutual reinforcements between safety and cybersecurity that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures.

c) A change driven by safety considerations should be reviewed by staff responsible for cybersecurity.

d) A change driven by cybersecurity considerations should be reviewed by staff responsible for safety.

6.3.9 Decommissioning activities

a) As-built information, including system actual interfaces, should be available and analysed before starting decommissioning individual I&C systems to ensure that the overall cybersecurity and safety objectives of the plant are not compromised by the decommissioning of the system, or by the related steps of the process.

b) In particular, when decommissioning of individual I&C systems leads to temporary provisions in order to maintain the safe operations of the plant, those provisions may induce new cybersecurity issues which should be analysed and addressed if deemed relevant by this analysis.

6.4 Selected technical aspects of I&C systems constrained by safety and cybersecurity

6.4.1 General

The objective of 6.4.2 to 6.4.6 is to provide guidance or requirements on some aspects of I&C programmable digital system design and operation, when they are subject to both safety and cybersecurity constraints. They deal with common situations where safety and cybersecurity technical measures or requirements conflict, depend or reinforce each others. Potential confusion between safety and cybersecurity measures is also addressed.

6.4.2 Logical access control for HMIs of I&C programmable digital systems in control rooms

a) Password-based logical access control for the operators shall not be implemented on HMIs of I&C programmable digital systems which need immediate operator access for plant safety. Alternative access control measures, acceptable from a safety point of view, should be implemented.

NOTE Possible alternative access control measures include permission to physically access the control rooms based on a rigorous screening of personnel, access limitation to operational HMI software (e.g., to BIOS or to the operating system level), software with restricted input (e.g. only from predefined lists). Such alternative access control measures are of particular importance for control rooms which are not permanently staffed (e.g. remote shutdown station).

b) Account/node locking or delayed login after invalid access attempts should not be implemented for I&C programmable digital systems which need immediate operator access for plant safety. Alternative measures, acceptable from a safety point of view, should be implemented.

c) The management of access controls shall take account of specific operational needs with safety implications (e.g., maintenance during night shifts, beyond design basis conditions, nuclear emergencies).

Note that requirements of 6.4.2 are valid for I&C programmable digital systems, not for their maintenance digital tools.

6.4.3 Software modification

6.4.3.1 Cybersecurity-driven software modifications

a) Cybersecurity-driven software modifications (including the application of a software security update) are a type of software modifications and shall be treated accordingly, i.e. in accordance with Clause 11 of IEC 60880:2006 for software of I&C CB systems supporting category A functions, in accordance with 5.10 and 6.10 of IEC 62138:2004 for software of I&C CB systems supporting category B or C functions, and in accordance with relevant local procedures for I&C programmable digital systems not important to safety.

b) The decision to implement a cybersecurity-driven software modification shall be validated by personnel knowledgeable of the targeted systems, their usage and their safety implications, in conjunction with those who are accountable for those systems.

c) Tests shall be conducted to validate that a cybersecurity-driven software modification (including the application of a software security update) does not degrade system ability to ensure its functions important to safety.

d) When it is decided not to apply a software security update, whatever the reason (e.g., tests as per c) or because the change is not possible during operations):

– the vulnerability associated with this non-application shall be traced and managed with the appropriate level of confidentiality;

– a dedicated risk analysis shall characterise the risks associated with this decision;

– if the risk analysis identifies the need for compensating cybersecurity measures, their implementation shall be approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems.

6.4.3.2 Other software modifications

a) Analyses or tests shall be conducted to validate that a software modification, made for safety or other reasons not related to cybersecurity (e.g. reliability, new functionality), does not result in inadequate cybersecurity.

b) A software modification identified as degrading cybersecurity shall not be implemented on plant I&C systems except if the three following conditions are met:
   – a dedicated risk analysis has been conducted and the residual risks formally accepted;
   – the compensating cybersecurity measures potentially identified by the risk analysis (if any) have been approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems;
   – these approved compensating cybersecurity measures (if any) have been implemented.

6.4.4 Logging and audit capability

a) Local record generation, audit reduction and report generation capability intended for cybersecurity should be implemented as much as possible external to systems important to safety.

b) The failure messages generated by a programmable digital I&C equipment should be logged outside this equipment to support safety or cybersecurity analyses.

c) Any logical connectivity implemented to centrally manage systems and/or cybersecurity logs should not interfere with independence requirements imposed upon systems important to safety.

NOTE Among the different possible approaches, strictly unidirectional channels to push logs are beneficial both from a security and safety point of view.

d) Logging mechanisms should be preferably implemented and pre-configured so that no logging management (e.g., level of detail, selectivity of logged events) is needed during plant operation.

6.4.5 Use of cryptography by I&C systems

a) Cryptographic mechanisms may be used by I&C programmable digital systems, but they shall not adversely impact the required performance (including response time), effectiveness, reliability or operation of functions important to safety.

b) For systems important to safety, cryptographic mechanisms aimed at ensuring confidentiality should only be used when justified by a cybersecurity risk analysis.

NOTE 1 I&C environments are usually resource-constrained whereas cryptography is resource-consuming. Integrity and availability are usually more important than confidentiality in I&C environment. Moreover, the use of confidentiality-focused mechanisms involves additional complexity, latency, and potential failures which are antagonistic with safety. Of course, specific contexts and risk analysis results can involve confidentiality needs and lead to the implementation of confidentiality-focused mechanisms. Moreover, I&C related information involves in some cases security classification and use of such confidentiality mechanisms.

c) In the case of I&C systems needed for the real-time management of beyond design basis conditions and nuclear safety emergencies, confidentiality-focused mechanisms should only be used when they can be fully justified.

d) Any communication or data integrity control initially designed for safety or reliability purposes and later considered as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined by staff responsible for cybersecurity, taking into account context-relevant cyberattacks, to confirm its cybersecurity effectiveness.

NOTE 2 As an illustration, the effectiveness of integrity control mechanisms differs largely depending on the nature of the threats: a classical CRC (Cyclic Redundancy Check) code is appropriate with regards to random failures whereas it is inefficient against an attacker, who is able to change the data and recompute the CRC to

make the new data considered as valid. Integrity control or assurance mechanisms specifically tailored for cybersecurity would detect the modification in this case.

6.4.6 System availability and function continuity

a) Any control initially designed to protect availability of a system from a safety or reliability perspective and later considered as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined by staff responsible for cybersecurity, taking into account context-relevant cyberattacks, to confirm its cybersecurity effectiveness.

NOTE Availability mechanisms tailored to address non-malicious failures are in some cases completely inefficient against malicious threats. Redundant but non-diversified systems are generally of little help against a cyberattack, as the redundant system will be vulnerable to the same attack.

b) Redundancy and back-up of safety-related data (e.g. configuration, parameters) or of components may be considered as cybersecurity counter-measures only when explicit justifications of their efficiency with respect to the considered malevolent threats are given.

7 Organizational and operational issues

7.1 Governance and responsibilities

a) Both cybersecurity and safety should be represented at the senior management or board level of the organization.

7.2 Coordination between safety and cybersecurity staff during operations

a) For each I&C programmable digital system, all personnel liable to access the system for cybersecurity or safety reasons should be identified. When different staffs, including safety staff and cybersecurity staff, are to access the system, these accesses should be coordinated and the schedules for each optimised.

b) Interventions on I&C programmable digital systems should be authorized both from a cybersecurity point of view and from a safety point of view.

c) Those entities responsible for safety and cybersecurity shall put adequate controls in place to ensure that sub-contractor staff who are granted access to I&C programmable digital systems to perform specific tasks are adequately controlled. In some instances, this may require such staff to be accompanied by a responsible and knowledgeable representative of the system's owner.

d) When a cybersecurity event is detected on a system important to safety, safety impact and cybersecurity impact analyses shall be made.

7.3 Safety and cybersecurity culture

a) Awareness and demonstration activities on I&C programmable digital system cybersecurity threats should be organized for I&C safety staff, in order to help them understand the existence and the nature of such threats and the potential impacts on safety.

b) Reciprocally, staff in charge of cybersecurity should be trained on main safety concepts and associated principles.

c) Opportunities for I&C operators, I&C maintenance staff, safety staff and cybersecurity staff to come together and exchange information about their roles, their practices, their environments and the associated threats should be provided.

NOTE This sort of opportunities is potentially beneficial for cybersecurity threat assessment activities. However, information classification issues are likely to occur; their resolution in a balanced way is a condition to obtain the maximum benefit from such practices.

7.4 Emergency response management

a) Procedures and organisations shall be in place in order to evaluate rapidly and rigorously safety implications of cybersecurity attacks on I&C programmable digital systems.

b) Any cybersecurity response decided in a cybersecurity crisis management context shall be evaluated in terms of safety impact before enforcement.

c) Potential cybersecurity implications of safety events and related response associated to I&C programmable digital systems should be evaluated and managed. Safety shall however remain the priority.

d) Integrated emergency exercise combining both safety and cybersecurity issues should be organized in order to challenge and enhance collaboration between staffs in charge of I&C systems, those in charge of plant safety, and those in charge of cybersecurity (where separated).

e) I&C programmable digital system isolation features and procedures, established for cybersecurity purposes, shall be analyzed in terms of safety consequences before allowance for enforcement.

Annex A
(informative)

Rationale for, and notes related to, the scope of this document

A.1 General

This annex presents the reasons and rationale which have lead to the scope defined in Clause 1.

A.2 Inclusion of I&C programmable digital system not important to safety

This document being focused on the coordination between safety and cybersecurity, a narrower scope, strictly limited to systems important to safety, has been initially considered. The experts involved in the document development have finally decided to include in the scope I&C programmable digital systems not important to safety because:

– it is consistent with the scope of the IEC 62645, to which this document is affiliated;
– assessing the impacts of cyberattacks, including in terms of plant safety, involves a global perspective (for instance, a targeted cyberattack on configuration or maintenance tools can lead to consequences on safety, although these tools can be classified as not important to safety).

The issue of coordinating safety and cybersecurity is better addressed by considering both I&C programmable digital systems important to safety and those not important to safety.

A.3 Exclusion of physical security, room access control and site security surveillance systems

This exclusion is inherited from and consistent with IEC 62645. However, it does not deny that cybersecurity has clear dependencies on the security of the physical environment (e.g., physical protection, power, heating/ventilation/air-conditioning systems, etc.). It is recognized that efficient I&C programmable digital system cybersecurity can only be achieved based on a sound physical security and physical protection regime, complying with national laws and regulations. From an international perspective, the IAEA provides relevant guidance.

A.4 Exclusion of non-malevolent actions and events

In consistence with IEC 62645, cybersecurity relates to prevention of, detection of, and reaction to malicious acts by digital means (cyberattacks) on I&C programmable digital systems. It does not cover considerations related to non-malevolent actions and events such as accidental failures, natural events, or human errors (except for those degrading cybersecurity). Although such aspects are sometimes included in other normative contexts (e.g., in the ISO/IEC 27000 series, the IEC 62443 series or the NIST framework), these exclusions and the focus on the protection against cyberattacks have been decided to provide the maximum consistency and the minimum overlap with the existing nuclear standards and practices. If aspects such as accidental failures, human errors and natural events are of course of prime importance, they are already covered by other SC 45A documents and standards, and are not considered as cybersecurity related in this document (except for human errors degrading cybersecurity).

A.5 Exclusion of development tools and platforms

This document is limited to I&C programmable digital systems used in NPPs, including on-site maintenance and configuration tools. It does not apply directly to development tools and platforms, typically found at the supplier premises. However, development tools and platforms might be impacted by the present document, in order to make the developed I&C systems and architectures meet its requirements. This exclusion does not deny the importance of securing development tools and platforms from a global cybersecurity perspective; it reflects the fact that this document has not been particularly developed to treat these aspects, which deserve due care but are to be treated mostly by non-nuclear specific provisions.

Bibliography

Nuclear I&C system specific references

MDEP, Common Position No. DICWG08, *Common position on the impact of cyber security features on digital I&C safety systems*

IAEA, Nuclear Security Series No. 17, Reference Manual, *Computer security at nuclear facilities*

ORNL, report ref. ORNL/NRC/LTR-07/05, *Safety and non-safety communications and interactions in international nuclear power plants*, 2007

U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, *Cyber security programs for nuclear facilities*, January 2010

U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, Rev. 3, 2011

IEEE, Std 7-4.3.2-2010, *Standard criteria for digital computers in safety systems of nuclear power generating stations*

CSA N290.7 Standard, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities*, 2014

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems in Nuclear Power Plants*

Interface between nuclear safety and nuclear security

IAEA, INSAG-24, *The interface between safety and security at nuclear power plants*

U.S. Nuclear Regulatory Commission, RG 5.74, *Managing the safety-security interface*

WINS, *An integrated approach to nuclear safety and nuclear security*, Rev. 1-1

Non-nuclear I&C system specific references

ISA TR84.00.09-2013, *Security protection layers and considerations related to SIS*

IEC 62443 (all parts), *Security for industrial automation and control systems*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

Non I&C-specific IAEA references

IAEA, GS-R-3:2006, *The management system for facilities and activities*

IAEA, Safety Guide No, GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA, Safety Guide No, GS-G-3.5:2009, *Management system for nuclear installations*

IAEA, Safety Standard Series No. SSR-2/1:2012, *Safety of Nuclear Power Plant: Design*

IAEA, Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants*

IAEA, Safety Guide SSG-34, *Design of electrical power systems in Nuclear Power Plants*

IAEA, Safety Glossary, *Terminology used in nuclear safety and radiation protection*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters
389 Chiswick High Road London W4 4AL UK