BS EN 16590-4:2014

BSI Standards Publication

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems

Part 4: Production, operation, modification and supporting processes (ISO 25119-4:2010 modified)

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 16590-4:2014. It supersedes BS ISO 25119-4:2010 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AGE/6, Agricultural tractors and forestry machinery.

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.

ISBN 978 0 580 82331 2

ICS 35.240.99; 65.060.01

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 April 2014.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16590-4

April 2014

ICS 35.240.99; 65.060.01

English Version

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 4: Production, operation, modification and supporting processes (ISO 25119-4:2010 modified)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien (ISO 25119-4:2010 modifié)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse (ISO 25119-4:2010 modifiziert)

This European Standard was approved by CEN on 23 February 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

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

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

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (EN 16590-4:2014) has been prepared by Technical Committee CEN/TC 144 “Tractors and machinery for agriculture and forestry”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2014, and conflicting national standards shall be withdrawn at the latest by October 2014.

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

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For relationship with EU Directive(s), see informative Annex ZA, which is an integral part of this document.

EN 16590 *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems* consists of the following parts:

— *Part 1: General principles for design and development*

— *Part 2: Concept phase*

— *Part 3: Series development, hardware and software*

— *Part 4: Production, operation, modification and supporting processes*

The modifications to ISO 25119-4:2010 are indicated by a vertical line in the margin.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

EN 16590 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising electrical and/or electronic and/or programmable electronic systems (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety, etc.).

The control system parts of the machines concerned are frequently assigned to provide the critical functions of the *safety-related parts of control systems* (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely critical functions or form part of an operational function.

In general, the designer (and to some extent, the user) will combine the design and validation of these SRP/CS as part of the risk assessment. The objective is to reduce the risk associated with a given hazard (or hazardous situation) under all conditions of use of the machine. This can be achieved by applying various protective measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

EN 16590 allocates the ability of safety-related parts to perform a critical function under foreseeable conditions into five performance levels. The performance level of a controlled channel depends on several factors, including system structure (category), the extent of fault detection mechanisms (diagnostic coverage), the reliability of components (mean time to dangerous failure, common-cause failure), design processes, operating stress, environmental conditions and operation procedures. Three types of failures are considered: systematic, common-cause and random.

In order to guide the designer during design, and to facilitate the assessment of the achieved performance level, EN 16590 defines an approach based on a classification of structures with different design features and specific behaviour in case of a fault.

The performance levels and categories can be applied to the control systems of all kinds of mobile machines: from simple systems (e.g. auxiliary valves) to complex systems (e.g. steer by wire), as well as to the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

EN 16590 adopts a risk-based approach for the determination of the risks, while providing a means of specifying the required performance level for the safety-related functions to be implemented by E/E/PES safety-related channels. It gives requirements for the whole safety life cycle of E/E/PES (design, validation, production, operation, maintenance, decommissioning), necessary for achieving the required functional safety for E/E/PES that are linked to the performance levels.

The structure of safety standards in the field of machinery is as follows.

a) Type-A standards (basic safety standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:

− type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

− type-B2 standards on safeguards (e.g. two-hand controls, interlocking devices, pressure sensitive devices, guards).

c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This part of EN 16590 is a type-B1 standard as stated in EN ISO 12100.

For machines which are covered by the scope of a machine specific type-C standard and which have been designed and built according to the provisions of that standard, the provisions of that type-C standard take precedence over the provisions of this type-B standard.

1 Scope

This part of EN 16590 provides general principles for the production, operation, modification and supporting processes of safety-related parts of control systems (SRP/CS) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It can also be applied to municipal equipment (e.g. street-sweeping machines). It specifies the characteristics and categories required of SRP/CS for carrying out their safety functions.

This part of EN 16590 is applicable to the safety-related parts of electrical/electronic/programmable electronic systems (E/E/PES), as these relate to mechatronic systems. It does not specify which safety functions, categories or performance levels are to be used for particular machines.

Machine specific standards (type-C standards) can identify performance levels and/or categories or they should be determined by the manufacturer of the machine based on risk assessment.

It is not applicable to non-E/E/PES systems (e.g. hydraulic, mechanic or pneumatic).

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 16590-1:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

EN 16590-2:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

EN 16590-3:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software*

ISO 3600, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Operator's manuals — Content and format*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 16590-1:2014 apply.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AGPL	agricultural performance level
$AGPL_r$	required agricultural performance level
CAD	computer-aided design
Cat	hardware category
CCF	common-cause failure
DC	diagnostic coverage
DC_{avg}	average diagnostic coverage
ECU	electronic control unit

ETA	event tree analysis
E/E/PES	electrical/electronic/programmable electronic systems
EMC	electromagnetic compatibility
EUC	equipment under control
FMEA	failure mode and effects analysis
FMECA	failure mode effects and criticality analysis
EPROM	erasable programmable read-only memory
FSM	functional safety management
FTA	fault tree analysis
HAZOP	hazard and operability study
HIL	hardware in the loop
MTTF	mean time to failure
$MTTF_d$	mean time to dangerous failure
PES	programmable electronic system
QM	quality measures
RAM	random-access memory
SOP	start of production
SRL	software requirement level
SRP	safety-related parts
SRP/CS	safety-related parts of control systems
SRS	safety-related system

5 Configuration management

5.1 Objectives

The first objective is to ensure that the SRP/CS and associated documents for a given function can be uniquely identified and reproduced at any time.

The second objective is to ensure that the relations and differences between earlier and current versions of the SRP/CS and associated documents can be traced.

5.2 General

All EN 16590 work products shall be handled by a configuration management system.

5.3 Prerequisites

See the prerequisites for each phase of the safety life cycle.

5.4 Requirements

Software tools and software development environments shall be subject to configuration management.

Configuration management data shall be maintained in accordance with a company document retention policy.

5.5 Work products

The applicable work product is the listing of SRP/CS with reference to associated documents for a given configuration.

6 Verification and validation

6.1 Objectives

One objective is to provide proof that the safety-related requirements are appropriate for the E/E/PES system and have duly been met.

A further objective is to provide proof that the safety goals at the machine level are satisfied.

6.2 General

The purpose of the preceding verification stages (e.g. reviews, safety analyses, component integration tests) was to demonstrate that the results of each particular phase complied with the relevant design and specification requirements described in EN 16590-3.

6.3 Prerequisites

The following are the prerequisites for this phase:

— project plan according to EN 16590-1:2014, 5.4.7 — deadlines, resources, equipment, degree of maturity, etc.;

— machine test plan — part of the existing quality assurance process;

— risk analysis according to EN 16590-2:2014, Clause 6 — identification of potential hazards;

— safety goals, as well as safe states;

— technical safety concept according to EN 16590-3:2014, Clause 5 — technical safety requirements.

6.4 Requirements

6.4.1 SRP design validation/verification

The design of the SRP of the control system shall be validated/verified (see EN 16590-1:2014, Figure 1).

The validation/verification shall demonstrate that each SRP meets

— all the requirements of the specified category (see EN 16590-2:2014, Annex A), and

— the specified safety characteristics for that part as set out in the design requirements.

6.4.2 Scope of safety validation/verification

Within the safety life cycle, validation/verification of safety attributes shall be carried out for the following:

— complete system at machine level (e.g. bench testing, hardware in the loop testing, test machine);

— hardware;

— software.

6.4.3 Activities

The following sequence shall be followed for a structured safety validation/verification:

— validation/verification planning;

— validation/verification specification;

— validation/verification execution;

— report on validation/verification result.

All variants or versions of the E/E/PES system that were subject to the validation/verification activities shall be clearly labelled.

6.4.4 Validation/verification plan

A validation/verification plan shall be developed for the safety goals and technical safety requirements, and shall include the following items:

— validation/verification and possible variants;

— degree of maturity of the system;

— validation/verification goals;

— validation/verification techniques;

— statement of independence between the person in charge of validation/verification and the developer;

— equipment and environmental conditions required, including calibration specifications for tools;

— specified reference to the overall project plan;

— pass/fail criteria for all tests.

6.4.5 Validation/verification, test specification of hardware and software

The item function shall be validated/verified at E/E/PES system level, considering fulfilment of the hardware/software safety requirements.

6.4.6 Validation/verification test specification of the complete system

The characteristics of the SRP/CS shall be validated/verified at machine level, considering fulfilment of the functional safety concept.

6.4.7 Validation/verification test specification

The following methods and measures shall be used and specified:

— tests (black-box, HIL, machine testing, field testing, etc.);

— analysis (e.g. simulation);

— reviews of relevant documents (input from hardware/software, e.g. FMEA, circuit diagram).

6.5 Work products

The following work products are applicable to this phase:

a) detailed validation/verification plan;

b) test specification;

c) validation/verification report that shall include proof that validation/verification goals have been met for

   1) the complete system at machine level,

   2) hardware, and

   3) software.

7 Product release

7.1 Objectives

The objective of this phase is to specify the conditions for product release as the completion of the E/E/PES systems development. Product release confirms that the requirements for functional safety in the machine have been met.

7.2 General

Figure 1 shows the approvals needed for an E/E/PES system development and the order of their completion that will satisfy the conditions for product release.

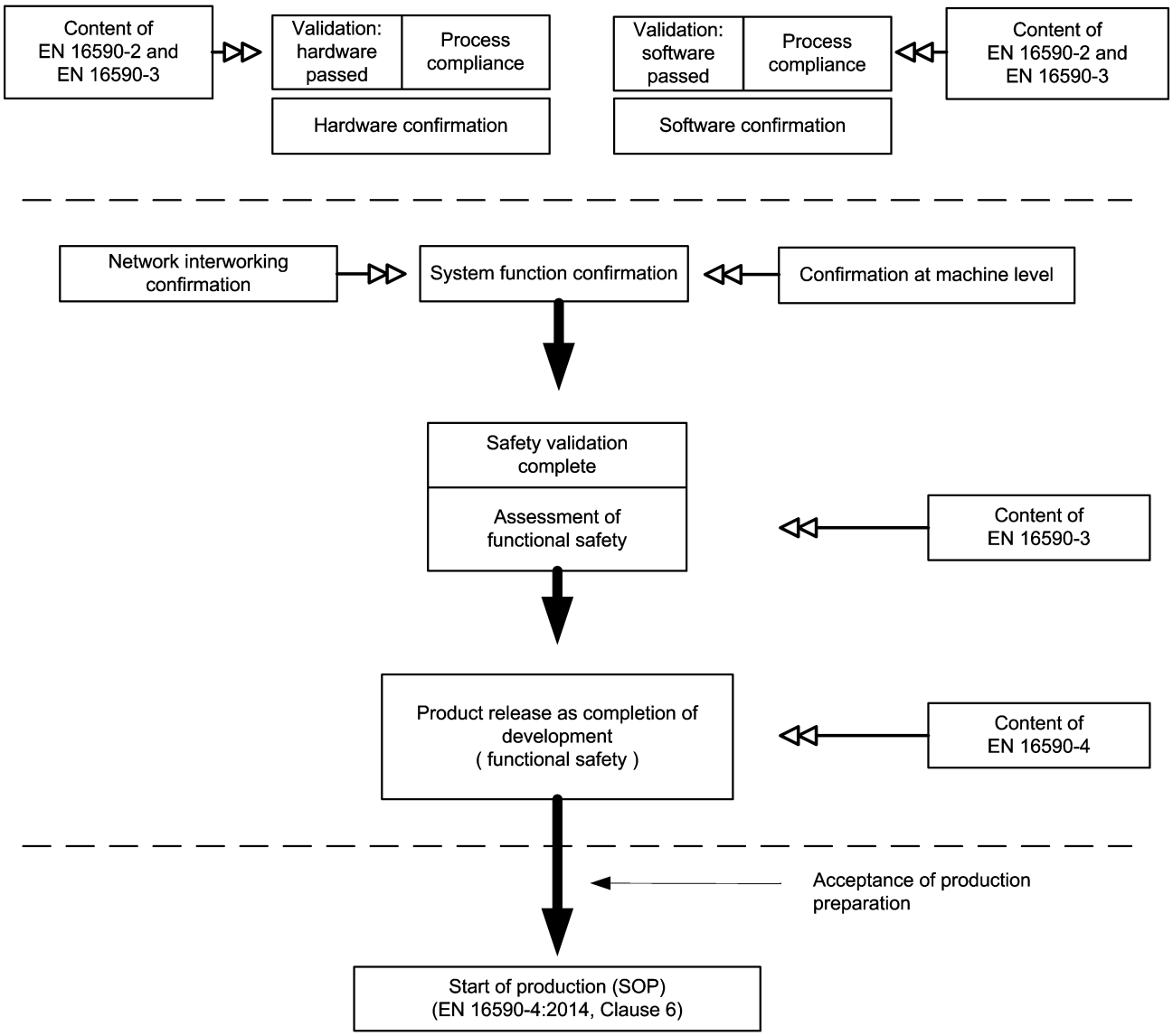

Figure 1 — Approval hierarchy

7.3 Prerequisites

The following are the prerequisites for this phase:

— confirmation report: hardware;

— confirmation report: software;

— confirmation report: machine level;

— assessment report on functional safety.

7.4 Requirements

7.4.1 Conditions for product release

Product release may only be approved if the following results are available from previous stages in the life cycle (see Annex A):

— an accepted assessment;

— hardware confirmation;

— software confirmation;

— system confirmation (including data parameterisation);

— confirmation at machine level;

— for the E/E/PES system, only when a release for the total machine is available.

7.4.2 Documentation of product release

Product release shall be documented and shall contain the following:

— name and signature of the person in charge of the release;

— version(s) of the released E/E/PES system;

— configuration of the released E/E/PES system;

— references to associated documents;

— release date.

NOTE The release document for functional safety could be part of the document for product release of the E/E/PES system or a separate document.

7.5 Work products

The applicable work product is the product release report document.

8 Production, production testing

8.1 Objectives

The objectives of this phase are to develop a production and installation plan for SRS, and to ensure that the required functional safety is maintained during the production process by the relevant product manufacturer, or person or organisation in charge of the process (machine manufacturer, supplier, sub-supplier, etc.).

8.2 General

By including safety-relevant characteristics in production planning and checking, this phase defines the steps required to ensure that functional safety is maintained during the production process as well.

8.3 Prerequisites

The following are the prerequisites for production and production testing:

— assembly notes (documentation of the parts or functions that can be affected by assembly);

— test notes;

— product release document;

— test criteria (safety-relevant characteristics to be tested);

— product monitoring — required for safety-relevant characteristics and ensuring that the safety-relevant characteristics of components are maintained in line with their specifications in the machine manufacturer's production process.

8.4 Requirements

8.4.1 Production plan

A production plan taking the assembly instructions into account shall include

— identification of safety-related characteristics;

— sequence and methods of production steps;

— assembly equipment/tools.

8.4.2 Production test plan

The test plan shall include

— identification of safety-related characteristics,

— sequence and methods of testing steps,

— test equipment/tools, test criteria, and

— production test frequency.

8.4.3 Personnel

Production and testing shall be carried out by trained personnel, according to the production and test plans.

8.4.4 Process capability

Process capability shall be ensured by means of standard industry requirements.

8.4.5 Documentation

The implementation of testing according to the test plan shall be documented. As a minimum, test documentation shall include test date, tester, unique part identification and test results.

8.4.6 Non-compliance

A procedure for non-compliance with a test criterion of SRP/CS shall be established. Reworking is permissible only upon proof of appropriate process control.

8.4.7 Storage and transport conditions

Any special handling and packaging requirements of SRP/CS shall be followed when storing and transporting the product.

8.5 Work products

The following work products are applicable to this phase:

a) documentation of tests performed according to the test plan;

b) non-compliance procedure;

c) storage and transport conditions.

9 Operation planning and maintenance (instructions for operating, servicing, repair, and decommissioning)

9.1 Objectives

The objective of this phase is to define the scope of the servicing, customer information and repair instructions of SRS, in order to maintain the required functional safety during operation, field observation, servicing, repair and decommissioning.

9.2 General

This clause presents the areas with safety-relevant characteristics relevant to the development of repair instructions and user information, and the planning, execution and monitoring of maintenance work.

9.3 Prerequisites

The following are the prerequisites for operation planning and maintenance:

— product release — release document regarding functional safety;

— quality management system (an implemented, routinely applied quality management system such as EN ISO 9001);

— maintenance notes — documentation of the safety-related areas that can be influenced through maintenance (maintenance tasks), and notes on experiences gathered through field analyses;

— configuration management plan — documented procedure for configuration management.

9.4 Requirements

9.4.1 General

The functional safety requirements during the maintenance and repair activities can be different from those required during operation.

9.4.2 Servicing schedule

A servicing schedule shall be prepared in parallel with the system design and shall include

— identification of components with safety-related characteristics, taking the relevant released subsystem or system configuration into account, and

— sequence, methods (tools, if necessary) and definition of the time interval and scope of servicing for the operating time to be defined.

9.4.3 Repair instructions

Repair instructions shall include

— identification of components with safety-related characteristics,

— work steps and workflow, methods and tools (e.g. programming and diagnostic equipment, if applicable),

— the relevant released configuration of the system or subsystem,

— permissible deactivation of subsystems or systems and the additional adjustments required on the complete machine, and

— spare parts supply with new parts or approved replacement parts.

9.4.4 Service technician instructions

Repair and servicing work shall

— be performed by appropriately trained personnel,

— be performed and documented according to the servicing schedule or repair instructions.

9.4.5 User information

User information (e.g. operating instructions) shall be prepared. Such operating instructions shall be included in the operator's manual in accordance with ISO 3600 and shall include

— identification of components with safety-related characteristics,

— warnings of potential hazards arising from the interaction with third-party products,

— description of subsystem or system and status information (display concept) and of the required customer reaction,

— description of the required components of servicing, and

— warnings against making modifications to the safety-related system (applies to AgPL = a to AgPL = e).

9.4.6 Field observation

A process of field observation shall be established. Appropriate measures based on the results of the analyses shall be initiated.

9.4.7 Storage and transport information

For the definition of storage and transport conditions of the product, safety-related characteristics for operating modes deviating from normal operation shall be taken into account (e.g. being towed, reduced driving operation).

9.4.8 Decommissioning and disassembling

The requirements regarding the decommissioning and disassembling of the machine shall be provided by the manufacturer.

9.5 Work products

The following work products are applicable to this phase:

a) repair instructions;

b) user instructions.

10 Modifications (change management)

10.1 General

In case of modifications to the product initiated by production, operation, field observation, servicing, repair or decommissioning of sub-functions, an impact analysis shall be used to decide which phases of the safety life cycle are to be repeated.

10.2 Objectives

The objective is to ensure that the functional safety system is appropriate, both during and after the modification and retrofit phase has taken place.

10.3 General

Change management helps to ensure systematic planning, controlling, monitoring, implementation and documentation of changes, while maintaining the consistency of all work products. Before changes are carried out, potential impacts on functional safety are assessed. For this purpose, decision-making processes for changes are introduced and established, with an assignment of responsibilities between the parties involved.

NOTE Here, “changes” are understood as *modifications* (corrections, removals, additions and enhancements, etc.).

10.4 Prerequisites

The following are the prerequisites for change management:

— project plan;

— configuration management plan.

10.5 Requirements

10.5.1 Product modification and improvement procedures

Procedures for carrying out any product modification or product improvement activity shall be described (standard operating procedure). An example of a modification procedure model is shown in Figure 2 and an example of an operation and maintenance management model is shown in Figure 3.

The product modification and product improvement phase shall be initiated only by the issue of an authorised request under the procedures for the management of functional safety (see EN 16590-1:2014, Clause 5).

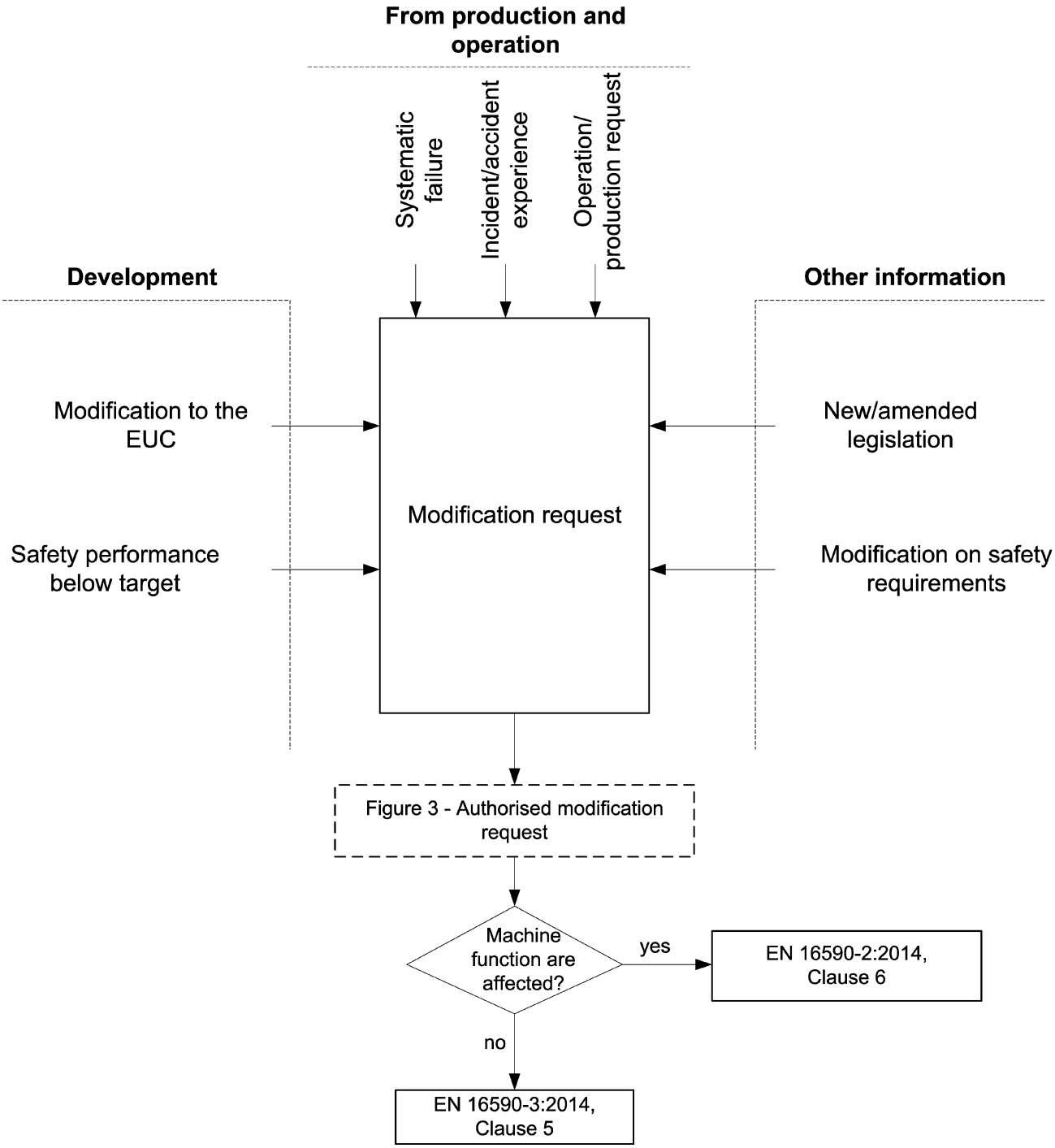

Figure 2 — Example modification procedure model

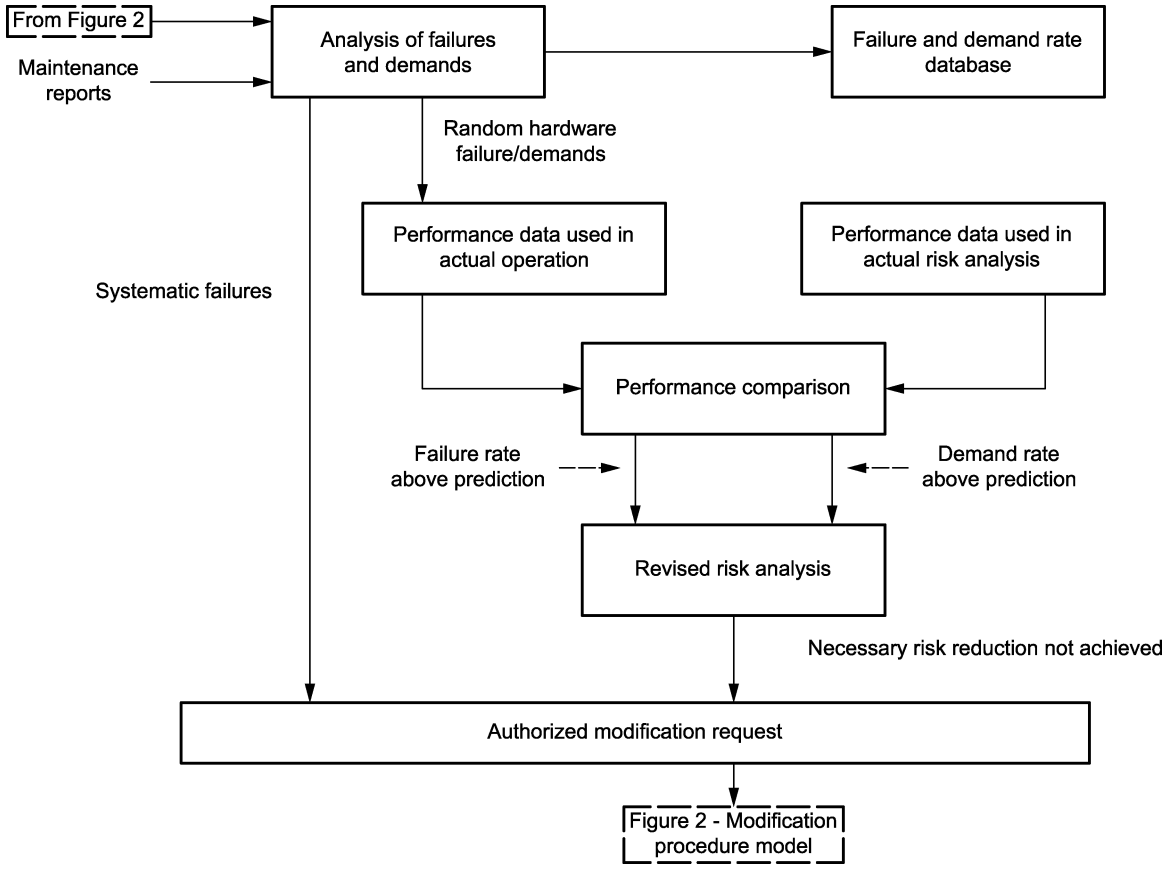

Figure 3 — Example operation and maintenance management model

10.5.2 Change request

The request shall detail the following:

a) the reasons for the change;

b) the proposed change (both hardware and software);

c) the determined hazards which could be affected (impact analysis);

d) compatibility across machines.

NOTE The reason for the request for the modification could arise from

— functional safety below that specified,

— systematic fault experience,

— new or amended safety legislation,

— modifications to the equipment under control or its use,

— modification to the overall safety requirements,

— analysis of operations and maintenance performance, indicating that the performance is below target,

— customer operation requests.

10.5.3 Assessing impact of modification

The responsible person shall decide whether the unit of observation has been modified to the extent of requiring a risk analysis (see EN 16590-2:2014, Clause 6), or whether the unit of observation has not been modified (see EN 16590-3:2014, Clause 5). This is determined after the impact analysis (see also Figure 2).

If the DC or MTTF for a channel is modified, then evaluation according to EN 16590-2:2014, Clause 6, is required. If there is no modification of DC or MTTF, but the micro-controller is changed (e.g. upgrading a micro-controller from 16 to 32 bit), then evaluation according to EN 16590-3:2014, Clause 6, is required.

The assessment shall also consider the impact of other concurrent product modification or product improvement activities.

Three modification examples follow, giving the required response in each case.

Change of a brake sensing function

If the brake sensing function is changed from dual- to single-channel, the classification of the category shall be reviewed. The development workflow shall then be continued from EN 16590-2:2014, Clause 7.

Change speed limit from 40 km/h to 50 km/h

The speed of a machine is increased from 40 km/h to 50 km/h, and different functions in the machine could be affected. This involves a complete re-assessment with respect to the risk analysis. The review shall then be started again in accordance with EN 16590-2:2014, Clause 5.

Controller upgrade

For the upgrade of a micro-controller from 16 bit to 32 bit without a change of the category, DC and MTTF for each channel, the point of continuation shall be EN 16590-3:2014, Clause 5.

NOTE 1 It can be necessary to implement a full hazard and risk analysis which could generate a need for performance levels that are different to those currently specified for the equipment under control.

NOTE 2 It cannot be assumed that the test procedures originally developed for final inspection can be reused without checking their validity.

10.5.4 Modification authorisation

Authorisation to carry out the required modification or retrofit activity shall be dependent on the results of the impact analysis.

10.6 Work products

The work product applicable to this phase is chronological documentation, which shall be established and maintained so that it gives details of all modifications and retrofits, including

— the modification or retrofit request,

— the impact analysis,

— reverification and revalidation of data and results, and

— all documents affected by the modification and retrofit activity.

11 Procedure for suppliers of SRS, subsystems and components

11.1 Objectives

The objective of this process is to describe the procedures and responsibilities within the relationship between machine manufacturers, suppliers and sub-suppliers of SRS for distributed developments.

11.2 General

The machine manufacturer and the suppliers for SRS shall jointly use the procedures of EN 16590. Responsibilities shall be clearly established between the machine manufacturer and the suppliers. Subcontractor relationships are permitted. Just as with the machine manufacturer, safety-related specifications concerning planning, execution and documentation for development, projects shall be established by all suppliers on distributed development projects, or development projects where the responsibility for safety is borne entirely by the supplier.

This does not apply for procurement of standard components, or development of supplied components that are not safety-related.

11.3 Prerequisites

The prerequisites for this phase are the following.

— Draft version of machine manufacturer/supplier development agreement: this agreement between the machine manufacturer and the supplier lays down the responsibilities for activities and work products.

— Supplier's quotation: these documents are of a general nature and therefore contain no prerequisite based on EN 16590.

11.4 Requirements

11.4.1 General

The activities relating the relationship between the machine manufacturer and supplier for distributed development shall encompass the following points; any necessary deviations shall be agreed upon:

— project initiation;

— project planning;

— project execution;

— assessment of functional safety;

— safety validation;

— documentation;

— confirmation measures;

— activities after SOP.

11.4.2 Scope of requirements

Machine manufacturer and supplier-related requirements apply to all items of a system being developed under EN 16590, except to primary components in the case where

a) there are no specific system safety-related requirements allocated to these primary components, or

b) technical and quality specifications of these primary components comply with the allocated system safety-related requirements.

11.4.3 Supplier selection

When selecting a supplier, the following shall be taken into account:

— assessment and documentation of whether the supplier has a quality management system in place;

— the supplier's experience and capability in developing SRP, subsystems, or systems — a documented process for functional safety management shall be checked, or this process can be jointly agreed between the machine manufacturer and the supplier.

When selecting a supplier, recommendations from the development, quality, and logistics department shall be considered.

11.4.4 Project initiation

When a project is initiated, persons in charge of functional safety for the project and sub-project shall be appointed for both the machine manufacturer and the supplier.

The machine manufacturer's project leader shall present the relevant parts of the machine manufacturer's product development process and functional safety process to the supplier.

It shall be decided in cooperation with the supplier which processes of EN 16590 are to be carried out. Work product responsibilities shall be clearly established.

The agreement between machine manufacturer and supplier shall also account for subcontractor relationships.

11.4.5 Project planning

The machine manufacturer and the supplier shall agree on a project plan, including milestones and key dates.

The machine manufacturer and the supplier shall both coordinate their quality assurance activities.

If the supplier places orders with subcontractors, the supplier shall manage these subcontractors in accordance with EN 16590 or a comparable standard.

The supplier shall develop a safety plan.

The machine manufacturer shall inform the supplier of all changes affecting functional and technical safety requirements. Such changes are subject to change management.

11.4.6 Project execution

Over the entire project term, the machine manufacturer and the supplier shall monitor and control product quality.

The supplier shall report to the machine manufacturer on all safety-related events, incidents and project-threatening risks that occur during project activities in its area of responsibility or in that of its subcontractors.

The supplier shall identify any safety goals that cannot be met. In this case, the safety concept shall be modified.

Any change introduced by the machine manufacturer or supplier that could affect the safety of the purchased system or planned measures to demonstrate compliance with EN 16590 shall be communicated to the other party for impact analysis.

11.4.7 Confirmation measures for the development partners' functional safety

The machine manufacturer and the supplier shall carry out an assessment of functional safety in all phases of the safety life cycle for which they are responsible.

The supplier shall report the results of the functional safety assessment to the machine manufacturer.

11.4.8 System validation

System validation shall be performed considering the integration requirements for the entire machine; the integration effort provided by the machine manufacturer shall be agreed upon.

Validation shall be performed and documented by the person in charge in accordance with project validation planning.

11.5 Work products

Documentation shall be compiled in accordance with EN 16590.

The supplier shall document the safety-related information obtained during planning, execution and completion of the project, to confirm that the product fulfils the safety requirements specified. The supplier shall provide the machine manufacturer with adequate documentation to complete his own documentation confirming that the product fulfils the safety requirements specified.

12 Technical documentation

12.1 Objectives

The objective is to provide required information (see Table A.1) in the form of documentation, so that every phase of the entire safety life cycle can be worked through effectively and can be reproduced.

12.2 Requirements

12.2.1 Document retention

The documentation shall be retained in accordance with company document retention policy on each phase of the entire safety life cycle needed for the effective completion of

— management of functional safety, and

— the carrying out of the assessment of functional safety.

NOTE 1 Only the information necessary for undertaking a particular activity, as required by EN 16590, need be held by each relevant party.

NOTE 2 This requirement assumes that company information retention policy is consistent with national legislation.

12.2.2 Document structure

The documentation shall

— be accurate and concise,

— be easy to understand by those persons having to make use of it,

— suit the purpose for which it is intended,

— be accessible and maintainable,

— be so structured as to make it possible to search for relevant information, and

— be such that it is possible to identify the latest revision (version).

The documentation requirements of this part of EN 16590 essentially concern information rather than physical documents. The information need not be contained in physical documents unless this is explicitly declared in the relevant subclause.

The individual items of the necessary documentation may be combined in one document.

Annex A
(informative)

Technical documentation checklist

Phase/measures		Reference to EN 16590
Management during complete safety life cycle		EN 16590-1:2014, Clause 5
	Verification measures Process instruction for auditing the processes during series development	EN 16590-1:2014, Table 2
	Safety plan	EN 16590-1:2014, 5.4.7.2
Assessment of functional safety		EN 16590-1:2014, Clause 6
	Verification measures (acceptance, conditional acceptance, rejection, open items) Responsible person	EN 16590-1:2014, 6.4.1
Concept — Definition of the unit of observation		EN 16590-2:2014, Clause 5
	Unit of observation and ambient conditions	EN 16590-2:2014, 5.3.1
	Limits of unit of observation and its interfaces with other units of observation	EN 16590-2:2014, 5.3.2
	Sources of stress	EN 16590-2:2014, 5.3.3
	Additional determinations	EN 16590-2:2014, 5.3.4
System design requirements		EN 16590-2:2014, Clause 7
	Safety function and associated $AgPL_r$	EN 16590-2:2014, 7.3.1
	Selected category	EN 16590-2:2014, Annex A
	Result of $MTTF_d$	EN 16590-2:2014, Annex B
	Result of DC	EN 16590-2:2014, Annex C
	Result of CCF	EN 16590-2:2014,Annex D
	Consideration of systematic failure avoidance	EN 16590-2:2014, Annex E
	Consideration of other typical functions	EN 16590-2:2014, Annex F
	Resulting SRL	EN 16590-2:2014, 7.4
System design		EN 16590-3:2014, Clause 5
	Functional safety concept (including other technical safety requirements, functional safety requirements, safety objectives, verification results, feasibility, consistency)	EN 16590-3:2014, 5.4.2 EN 16590-3:2014, 5.4.3
	Review report of functional safety requirements	EN 16590-3:2014, 5.4.2
	Environmental conditions Machine conditions Resulting AgPL Safe state description	EN 16590-3:2014, 5.4.2.2
	States and times	EN 16590-3:2014, 5.4.3.2.2
	Safety architecture, interfaces and marginal conditions	EN 16590-3:2014, 5.4.3.2.3

Phase/measures	Reference to EN 16590
Series development – Hardware	EN 16590-3:2014, Clause 6
Hardware safety validation test plan	EN 16590-3:2014, 6.6
Hardware safety validation test specification	EN 16590-3:2014, 6.6
Hardware safety validation test results	EN 16590-3:2014, 6.6
Hardware system integration test plan	EN 16590-3:2014, 6.6
Hardware system integration test specification	EN 16590-3:2014, 6.6
Hardware system integration test results	EN 16590-3:2014, 6.6
Series development – Software	EN 16590-3:2014, Clause 7
Software project plan	EN 16590-3:2014, 7.1.5
Software safety requirement specification	EN 16590-3:2014, 7.2.5
Non-safety related requirements specification	EN 16590-3:2014, 7.2.5
Acceptance criteria for software safety requirements	EN 16590-3:2014, 7.2.5
Verification report or the software safety requirements specification	EN 16590-3:2014, 7.2.5
Software architecture	EN 16590-3:2014, 7.3.5
Software architecture verification report	EN 16590-3:2014, 7.3.5
Detailed design of the software	EN 16590-3-:2014, 7.4.5
Software	EN 16590-3:2014, 7.4.5
Software verification report	EN 16590-3:2014, 7.4.5
Software module test plan	EN 16590-3:2014, 7.5.5
Software module test specification	EN 16590-3:2014, 7.5.5
Software module test report	EN 16590-3:2014, 7.5.5
Software integration test plan	EN 16590-3:2014, 7.6.5
Software integration test specification	EN 16590-3:2014, 7.6.5
Software integration test report	EN 16590-3:2014, 7.6.5
Software validation plan	EN 16590-3:2014, 7.7.5
Software validation test specification	EN 16590-3:2014, 7.7.5
Software validation test report	EN 16590-3:2014, 7.7.5
Release for SOP	EN 16590-4:2014, Clause 7
Product release report	EN 16590-4:2014, 7.4.2
Configuration management	EN 16590-4:2014, Clause 5
Listing of SRP/CS with reference to associated documents for a given configuration	EN 16590-4:2014, 5.4
Verification and validation	EN 16590-4:2014, Clause 6
Validation and verification plan	EN 16590-4:2014, 6.4.4
Test specification	EN 16590-4:2014, 6.4.7
Validation and verification report	EN 16590-4:2014, 6.5

Phase/measures		Reference to EN 16590
Production planning		EN 16590-1:2014, Clause 8
	Documentation of safety-related production steps (production plan)	EN 16590-1:2014, 8.4.1
	Testing and adjustment criteria (safety-related)	EN 16590-1:2014, 8.4.2
	Documentation of non-compliance	EN 16590-1:2014, 8.4.6
Production, production testing		EN 16590-1:2014, Clause 8 EN 16590-4:2014, Clause 8
	Documentation of tests performed according to test plan	EN 16590-4:2014, 8.4.5
	Non-compliance procedure	EN 16590-4:2014, 8.4.6
	Storage and transport conditions	EN 16590-4:2014, 8.4.7
	Traceability of products for safety related criteria	EN 16590-1:2014, 8.4.7
Maintenance (field monitoring, servicing, repair and decommissioning)		EN 16590-1:2014, 7.4.3 EN 16590-4:2014, 9.4
	Repair instructions	EN 16590-4:2014, 9.4.3
	User instructions	EN 16590-4:2014, 9.4.5
Modification/change management		EN 16590-4:2014, Clause 10
	Modification or retrofit request (authorised)	EN 16590-4:2014, 10.5.2
	Impact analysis	EN 16590-4:2014, 10.5.3
	Reverification and revalidation of data and results	EN 16590-4:2014, 10.6
	All documents affected by the modification and retrofit activity	EN 16590-4:2014, 10.6

Annex ZA
(informative)

Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association to provide a means of conforming to Essential Requirements of the New Approach Machinery Directive 2006/42/EC.

Once this standard is cited in the Official Journal of the European Union under that Directive and has been implemented as a national standard in at least one Member State, compliance with the normative clauses of this standard confers, within the limits of the scope of this standard, a presumption of conformity with the relevant Essential Requirements 1.2.1 and 1.7 of Annex I of that Directive and associated EFTA regulations.

NOTE Compliance with the normative clauses of parts 1, 2, 3 and 4 of EN 16590 is required to achieve the presumption of conformity indicated in this annex.

WARNING — Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this standard.

Bibliography

[1] EN ISO 9001:2008, *Quality management systems - Requirements (ISO 9001:2008)*

[2] EN ISO 12100, *Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010)*

[3] ISO 15003, *Agricultural engineering — Electrical and electronic equipment — Testing resistance to environmental conditions*

[4] ISO/TS 16949:2009, *Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations*

[5] EN 61000-4-1, *Electromagnetic compatibility (EMC) — Part 4-1: Testing and measurement techniques — Overview of IEC 61000-4 series (IEC 61000-4-1)*

[6] EN 61496-1, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests (IEC 61496-1)*

[7] *HSE Guidelines on Programmable Electronic Systems in Safety-related Applications,* Part 1 (ISBN 0 11 883906 6) and Part 2 (ISBN 0 11 883906 3)

This page deliberately left blank

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.

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 bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

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.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 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.

...making excellence a habit.™