INTERNATIONAL STANDARD

IEC 61511-1

First edition
2003-01

Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and software requirements

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le secteur des industries de transformation –

Partie 1:
Cadre, définitions et prescriptions concernant le système, le matériel et le logiciel

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

IEC

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XC

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.

3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.

4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.

6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control. The text of this standard is based on the following documents:

FDIS	Report on voting
65A/368/FDIS	65A/372/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.

IEC 61511 consists of the following parts, under the general title *Functional safety: Safety instrumented systems for the process industry sector* (see Figure 1):

- Part 1: Framework, definitions, system, hardware and software requirements
- Part 2: Guidelines in the application of IEC 61511-1
- Part 3: Guidance for the determination of the required safety integrity levels

The committee has decided that the contents of this publication will remain unchanged until 2007. At this date, the publication will be

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

A bilingual version of this standard may be issued at a later date.

INTRODUCTION

Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industries. If instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards and performance levels.

This international standard addresses the application of safety instrumented systems for the Process Industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This international standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This standard addresses safety instrumented systems which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This International Standard is process industry specific within the framework of IEC 61508 (see Annex A).

This International Standard sets out an approach for safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This International Standard on safety instrumented systems for the process industry

- addresses all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

This International Standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example, national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

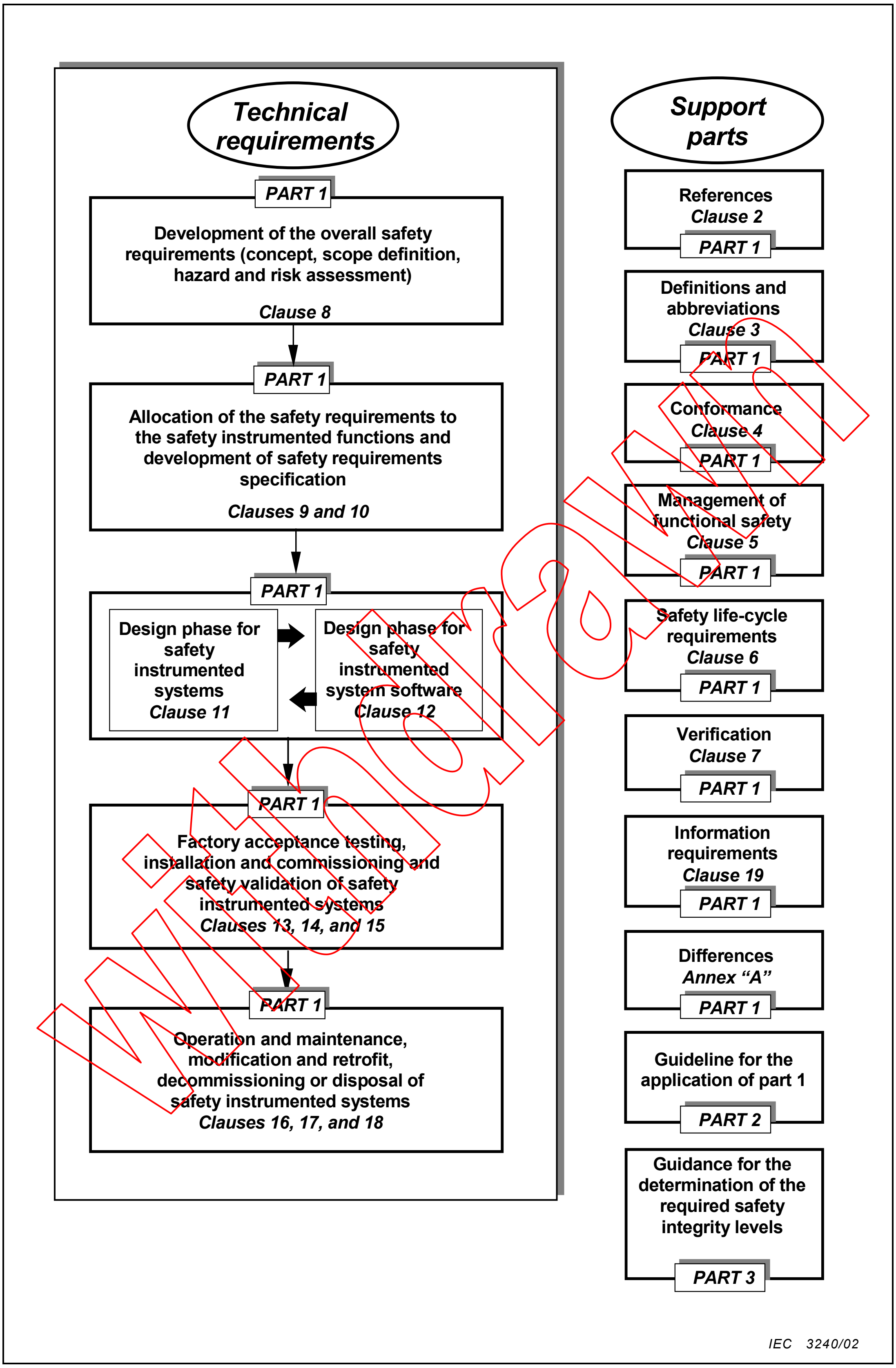

Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk assessment)
Clause 8
PART 1
Allocation of the safety requirements to the safety instrumented functions and development of safety requirements specification
Clauses 9 and 10
PART 1
Design phase for safety instrumented systems
Clause 11
Design phase for safety instrumented system software
Clause 12
PART 1
Factory acceptance testing, installation and commissioning and safety validation of safety instrumented systems
Clauses 13, 14, and 15
PART 1
Operation and maintenance, modification and retrofit, decommissioning or disposal of safety instrumented systems
Clauses 16, 17, and 18
Support parts
References
Clause 2
PART 1
Definitions and abbreviations
Clause 3
PART 1
Conformance
Clause 4
PART 1
Management of functional safety
Clause 5
PART 1
Safety life-cycle requirements
Clause 6
PART 1
Verification
Clause 7
PART 1
Information requirements
Clause 19
PART 1
Differences
Annex "A"
PART 1
Guideline for the application of part 1
PART 2
Guidance for the determination of the required safety integrity levels
PART 3
IEC 3240/02

Figure 1 – Overall framework of this standard

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

1 Scope

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.

In particular, this standard

a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility will be assigned to different parties according to safety planning and national regulations;

b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of IEC 61511-1, is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);

c) defines the relationship between IEC 61511 and IEC 61508 (Figures 2 and 3);

d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);

e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;

NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.

f) outlines the relationship between safety instrumented functions and other functions (Figure 4);

g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;

h) specifies requirements for system architecture and hardware configuration, application software, and system integration;

i) specifies requirements for application software for users and integrators of safety instrumented systems (clause 12). In particular, requirements for the following are specified:

- safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;
- information relating to the software safety validation to be passed to the organization carrying out the SIS integration;

- preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications to safety software;

j) applies when functional safety is achieved using one or more safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment;

k) may be applied in non-safety applications such as asset protection;

l) defines requirements for implementing safety instrumented functions as a part of the overall arrangements for achieving functional safety;

m) uses a safety life cycle (Figure 8) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems;

n) requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

NOTE See Figure 9 for an overview of risk reduction methods.

o) establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels;

p) specifies minimum requirements for hardware fault tolerance;

q) specifies techniques/measures required for achieving the specified integrity levels;

r) defines a maximum level of performance (SIL 4) which can be achieved for a safety instrumented function implemented according to this standard;

s) defines a minimum level of performance (SIL 1) below which this standard does not apply;

t) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications (which should be established based on knowledge of the particular application);

u) specifies requirements for all parts of the safety instrumented system from sensor to final element(s);

v) defines the information that is needed during the safety life cycle;

w) requires that the design of a safety instrumented function takes into account human factors;

x) does not place any direct requirements on the individual operator or maintenance person.

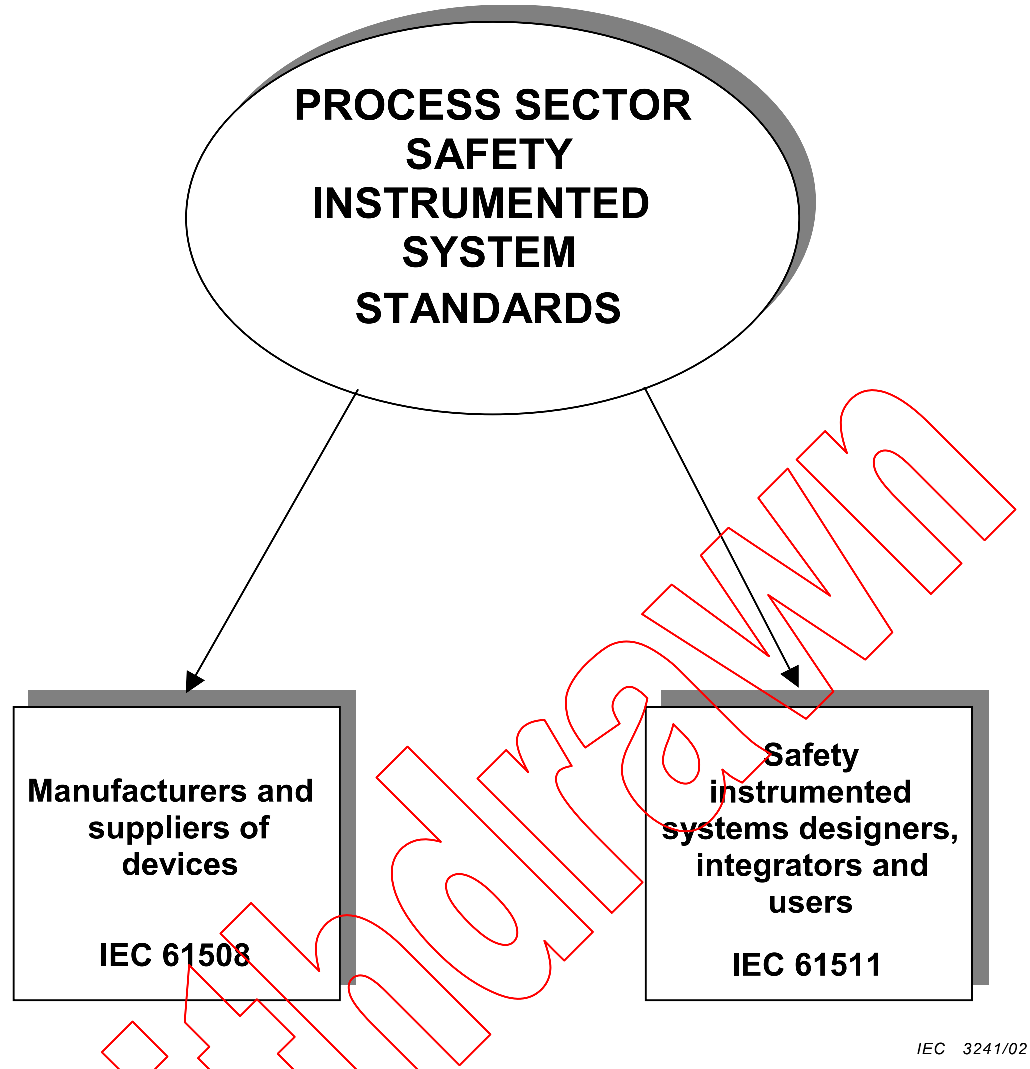
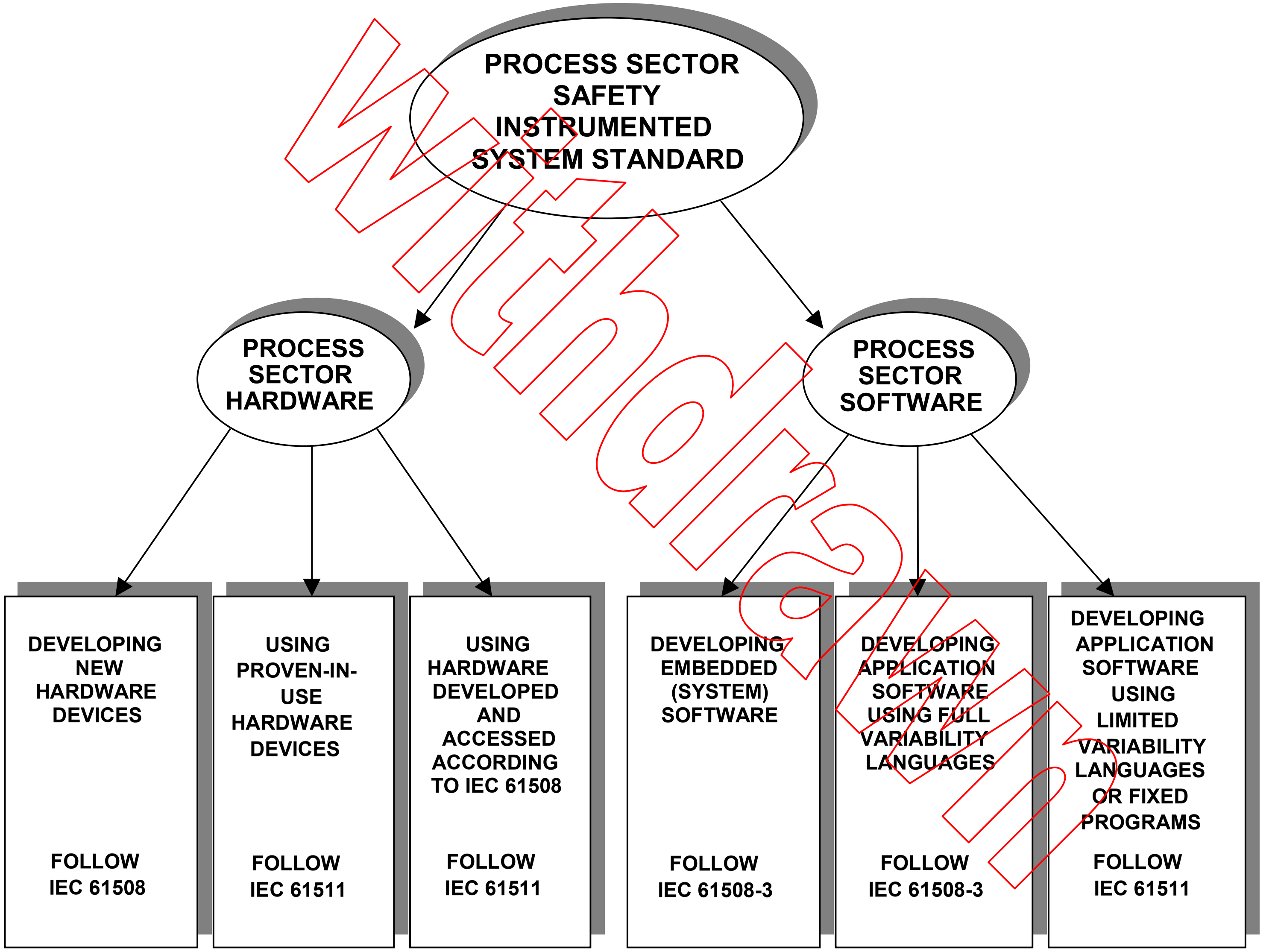

PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARDS
Manufacturers and suppliers of devices
IEC 61508
Safety instrumented systems designers, integrators and users
IEC 61511
IEC 3241/02

Figure 2 – Relationship between IEC 61511 and IEC 61508


PROCESS SECTOR SAFETY INSTRUMENTED SYSTEM STANDARD
PROCESS SECTOR HARDWARE
PROCESS SECTOR SOFTWARE
DEVELOPING NEW HARDWARE DEVICES
FOLLOW IEC 61508
USING PROVEN-IN-USE HARDWARE DEVICES
FOLLOW IEC 61511
USING HARDWARE DEVELOPED AND ACCESSED ACCORDING TO IEC 61508
FOLLOW IEC 61511
DEVELOPING EMBEDDED (SYSTEM) SOFTWARE
FOLLOW IEC 61508-3
DEVELOPING APPLICATION SOFTWARE USING FULL VARIABILITY LANGUAGES
FOLLOW IEC 61508-3
DEVELOPING APPLICATION SOFTWARE USING LIMITED VARIABILITY LANGUAGES OR FIXED PROGRAMS
FOLLOW IEC 61511

IEC 3242/02

Figure 3 – Relationship between IEC 61511 and IEC 61508 (see clause 1)

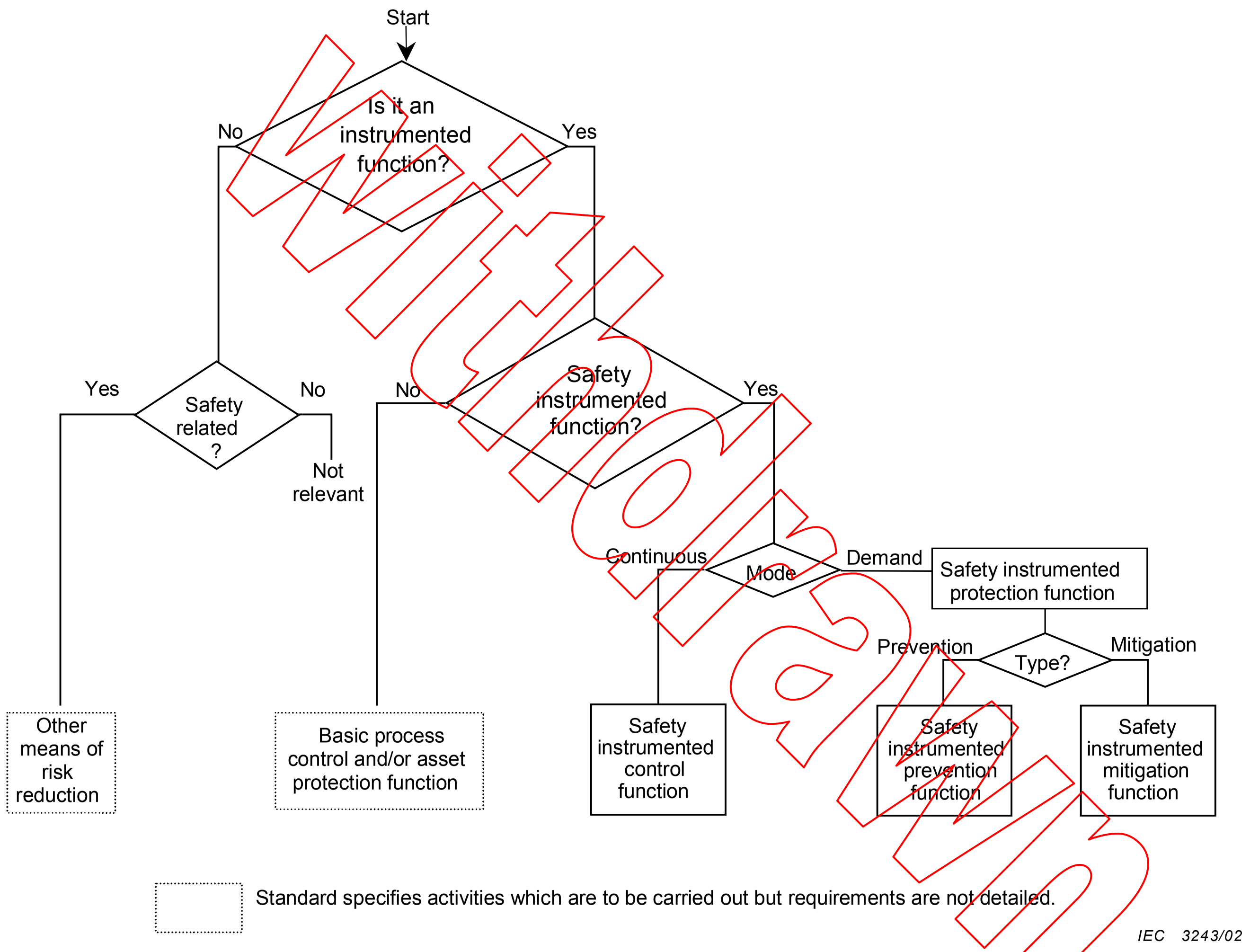
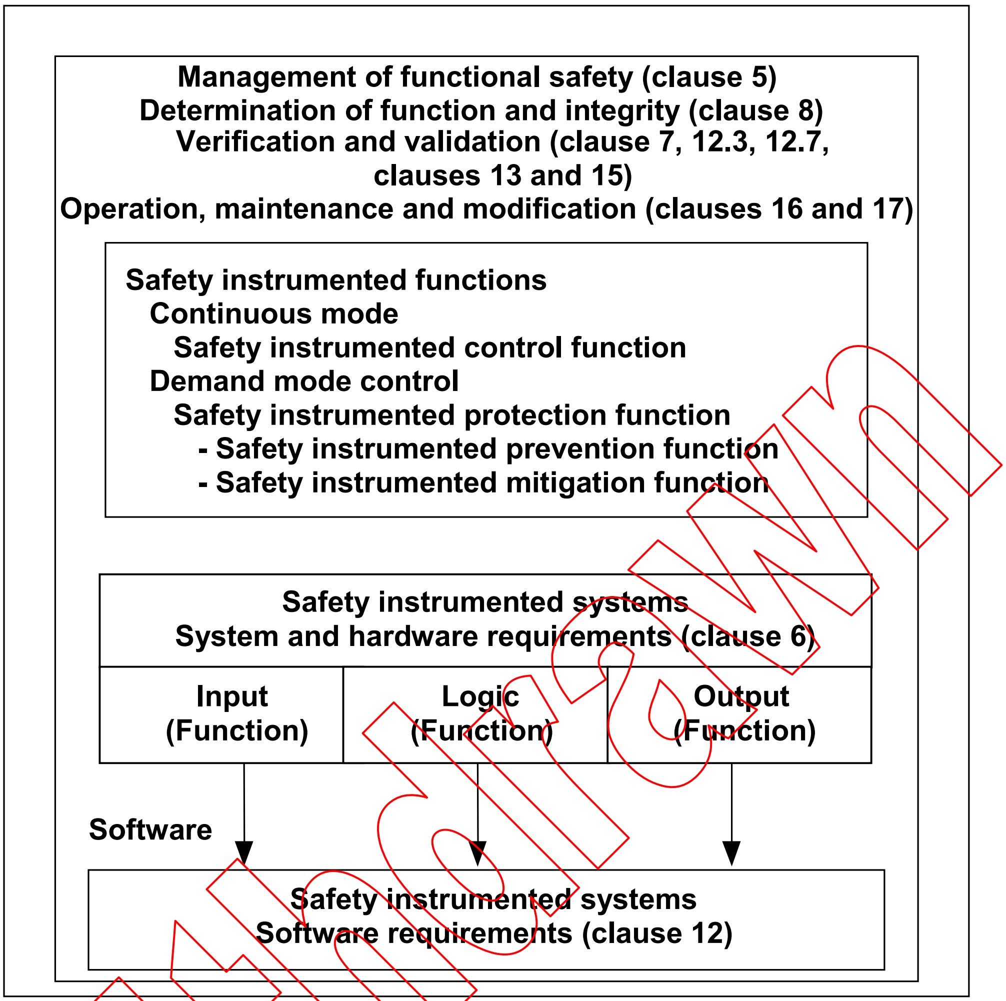

Start
Is it an instrumented function?
No
Yes
Safety related ?
Yes
No
Not relevant
Safety instrumented function?
No
Yes
Mode
Continuous
Demand
Safety instrumented protection function
Type?
Prevention
Mitigation
Other means of risk reduction
Basic process control and/or asset protection function
Safety instrumented control function
Safety instrumented prevention function
Safety instrumented mitigation function
Standard specifies activities which are to be carried out but requirements are not detailed.
IEC 3243/02

Figure 4 – Relationship between safety instrumented functions and other functions


Management of functional safety (clause 5)
Determination of function and integrity (clause 8)
Verification and validation (clause 7, 12.3, 12.7, clauses 13 and 15)
Operation, maintenance and modification (clauses 16 and 17)
Safety instrumented functions
Continuous mode
Safety instrumented control function
Demand mode control
Safety instrumented protection function
- Safety instrumented prevention function
- Safety instrumented mitigation function
Safety instrumented systems
System and hardware requirements (clause 6)
Input (Function)
Logic (Function)
Output (Function)
Software
Safety instrumented systems
Software requirements (clause 12)

IEC 3244/02

Figure 5 – Relationship between system, hardware, and software of IEC 61511-1

2 Normative references

The following referenced documents are indispensable for the application 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 60654-1:1993, *Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions*

IEC 60654-3:1998, *Industrial-process measurement and control equipment – Operating conditions – Part 3: Mechanical influences*

IEC 61326-1:*Electrical equipment for measurement, control and laboratory use – EMC requirements*

IEC 61508, *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 61511-2: *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines in the application of IEC 61511-1*[1]

[1] To be published.