SVENSK STANDARD SS-EN 61511-1

Fastställd	Utgåva	Sida	Ansvarig kommitté
2005-09-26	1	1 (1+89)	SEK TK 65

Funktionssäkerhet – Säkerhetskritiska system för processindustrin – Del 1: Allmänt, definitioner samt fordringar på system, maskinvara och programvara

Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

Som svensk standard gäller europastandarden EN 61511-1:2004. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61511-1:2004.

Nationellt förord

Europastandarden EN 61511-1:2004[*)]

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC

– **IEC 61511-1, First edition, 2003**[**)] **- Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements**

utarbetad inom International Electrotechnical Commission, IEC.

[*)] EN 61511-1:2004 ikraftsattes 2005-09-26 som SS-EN 61511-1 genom offentliggörande, d v s utan utgivning av något svenskt dokument.

[**)] Corrigendum, November 2004 till IEC 61511-1:2003, påverkar endast den franska titeln.

ICS 13.110; 25.040.01

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

EUROPEAN STANDARD **EN 61511-1**

NORME EUROPÉENNE

EUROPÄISCHE NORM December 2004

ICS 13.110; 25.040.01

English version

Functional safety – Safety instrumented systems for the process industry sector Part 1: Framework, definitions, system, hardware and software requirements

(IEC 61511-1:2003 + corrigendum 2004)

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel (CEI 61511-1:2003 + corrigendum 2004)

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003 + Corrigendum 2004)

This European Standard was approved by CENELEC on 2004-10-01. CENELEC 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 Central Secretariat or to any CENELEC 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 CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 61511-1:2004 E

SEK Svensk Elstandard

Foreword

The text of the International Standard IEC 61511-1:2003, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61511-1 on 2004-10-01 without any modification.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2005-10-01

– latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2007-10-01

Annex ZA has been added by CENELEC.

_____

Endorsement notice

The text of the International Standard IEC 61511-1:2003 + corrigendum November 2004 was approved by CENELEC as a European Standard without any modification.

_____

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE Where an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 60654-1	1993	Industrial-process measurement and control equipment - Operating conditions Part 1: Climatic conditions	EN 60654-1	1993
IEC 60654-3	1983	Part 3: Mechanical influences	EN 60654-3	1997
IEC 61326	- [1)]	Electrical equipment for measurement, control and laboratory use - EMC requirements	EN 61326	1997 [2)]
IEC 61508-2	- [1)]	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001 [2)]
IEC 61508-3	- [1)]	Part 3: Software requirements	EN 61508-3	2001 [2)]
IEC 61511-2	- [1)]	Functional safety - Safety instrumented systems for the process industry sector Part 2: Guidelines for the application of IEC 61511-1	EN 61511-2	2004 [2)]

1) Undated reference.

2) Valid edition at date of issue.

CONTENTS

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 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 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 standard is process industry specific within the framework of IEC 61508 (see Annex A).

This 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 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.

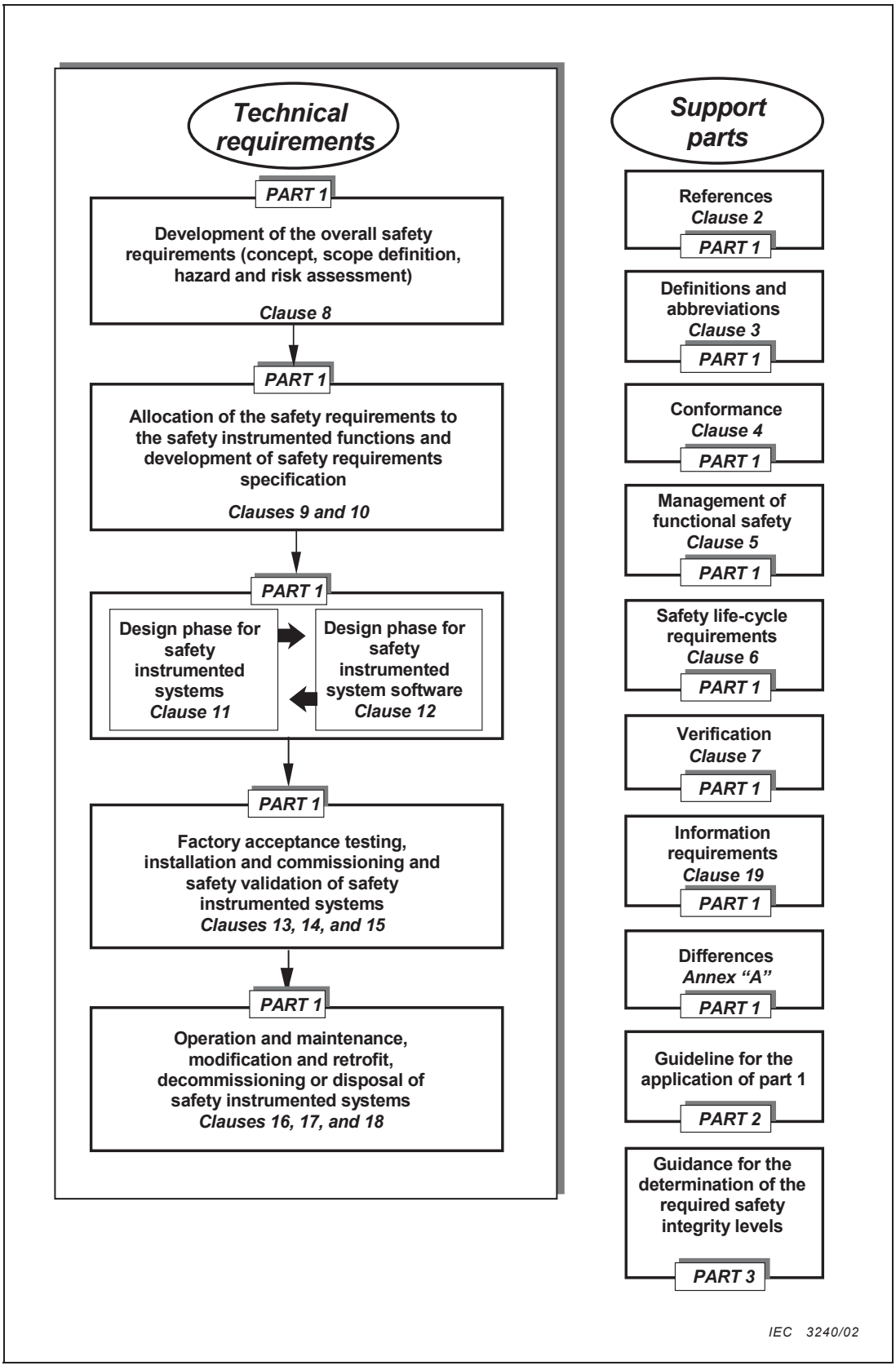


Figure 1 – Overall framework of this standard

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.

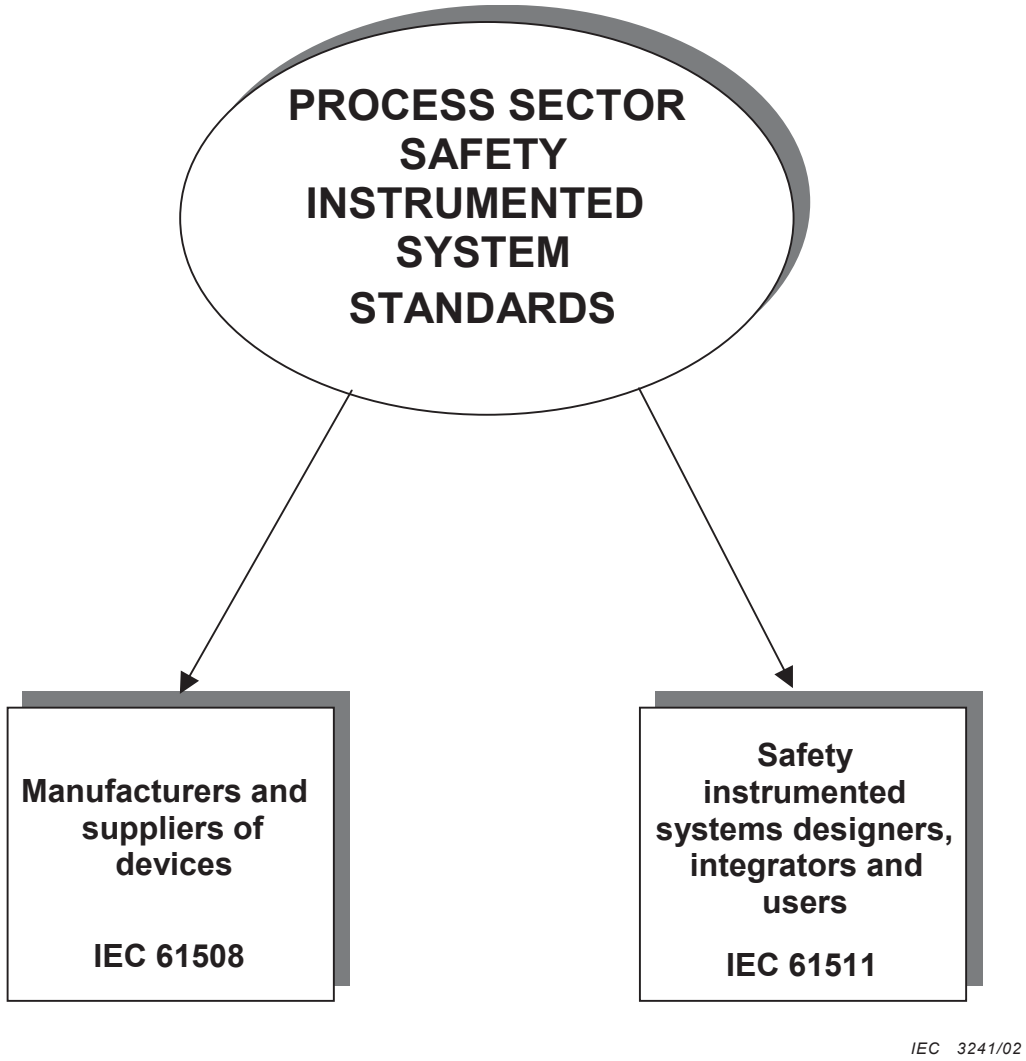


Figure 2 – Relationship between IEC 61511 and IEC 61508

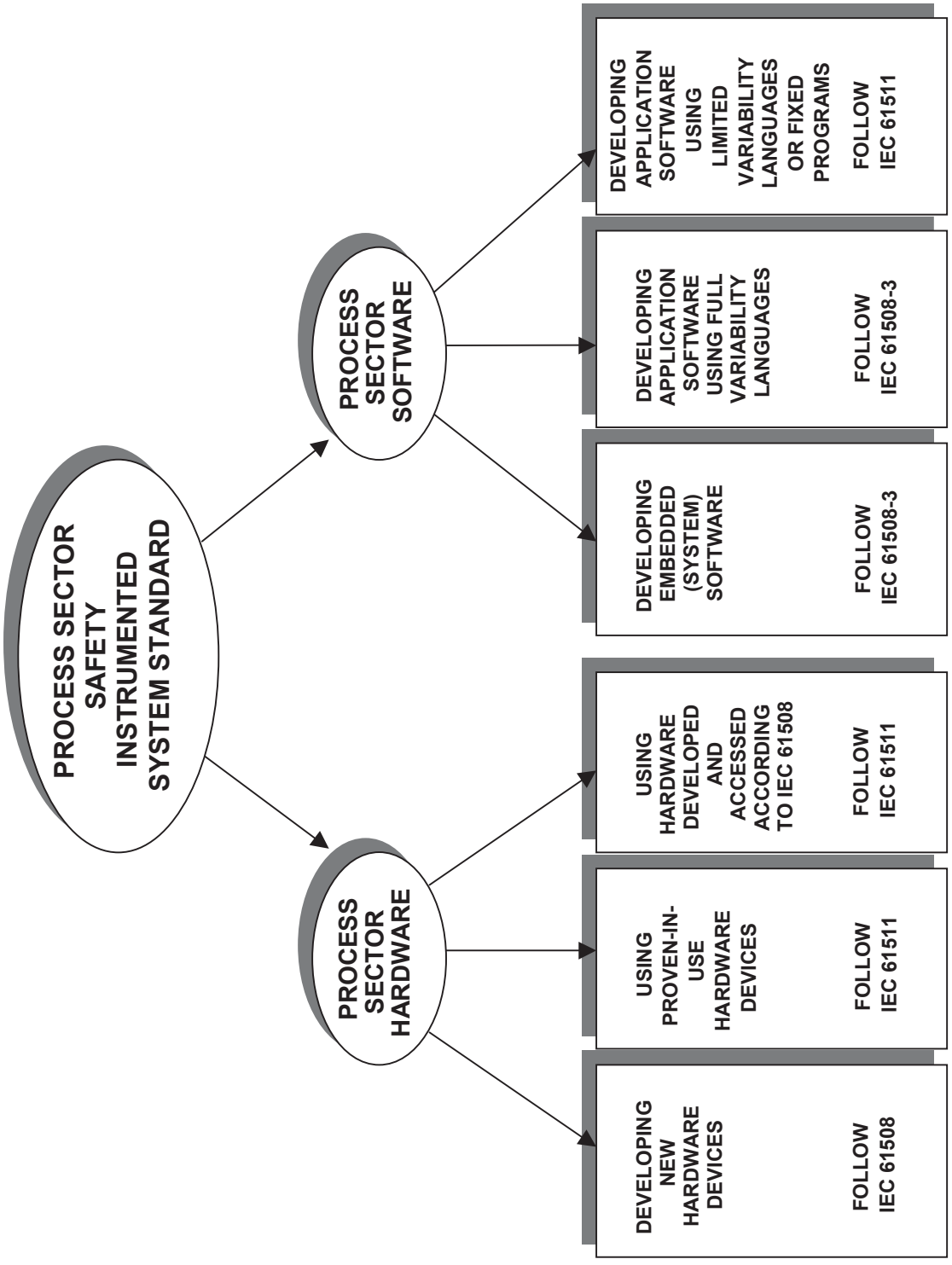


Figure 3 – Relationship between IEC 61511 and IEC 61508 (see clause 1)

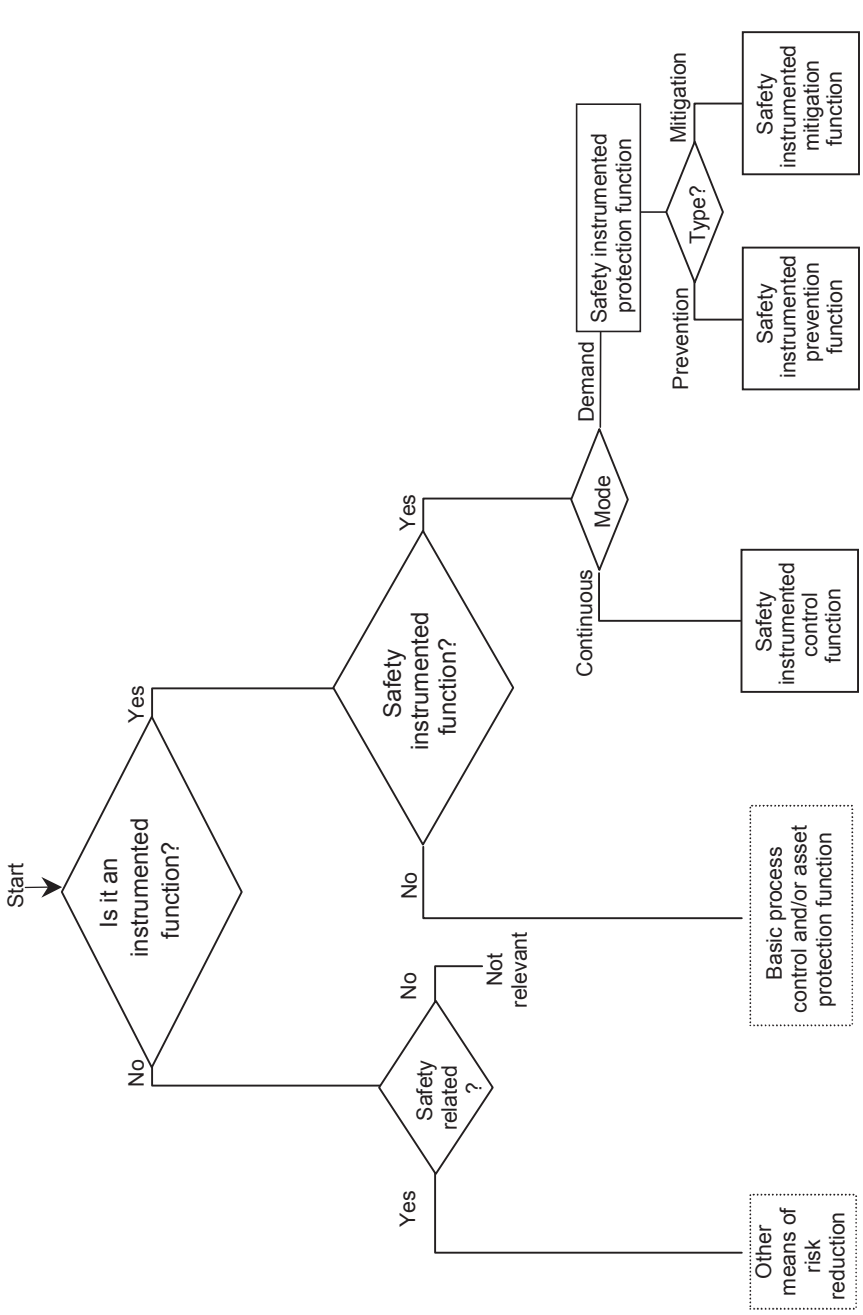
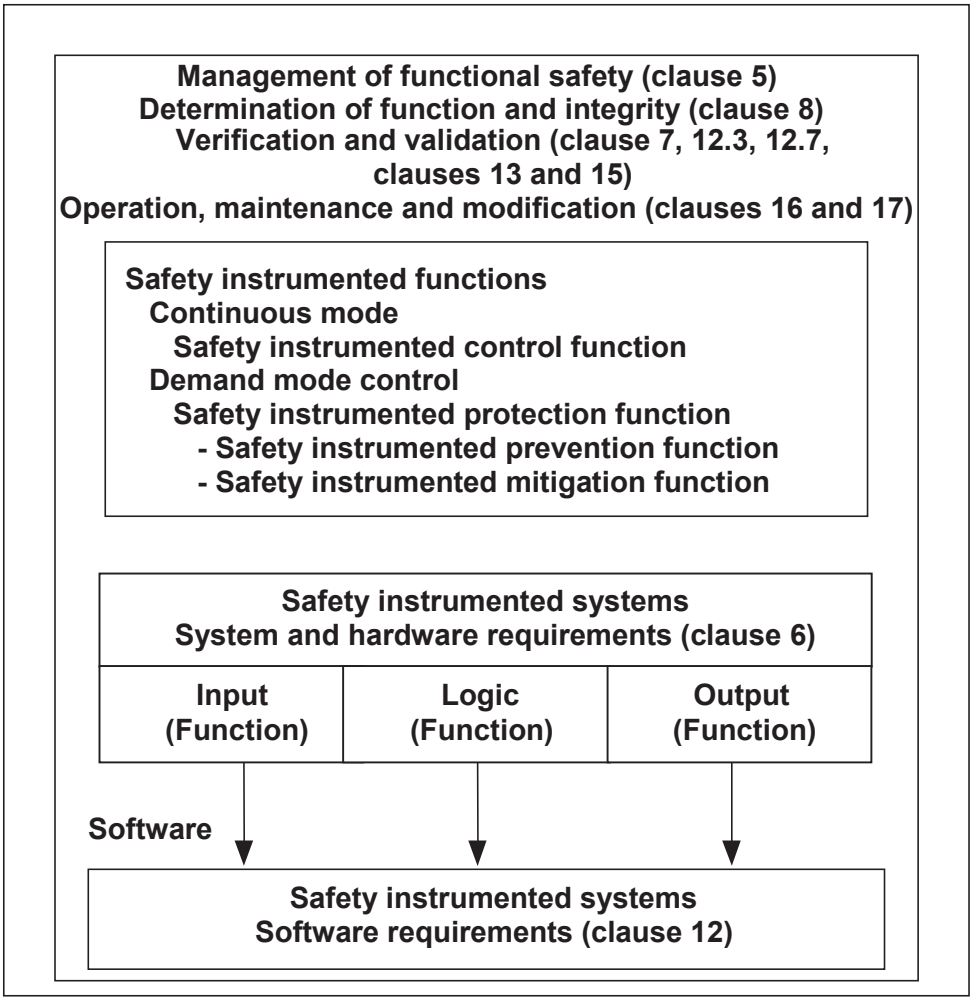


Figure 4 – Relationship between safety instrumented functions and other functions



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