SVENSK STANDARD SS-EN 61511-3

Fastställd	Utgåva	Sida	Ansvarig kommitté
2005-09-26	1	1 (1+57)	SEK TK 65

Funktionssäkerhet – Säkerhetskritiska system för processindustrin – Del 3: Vägledning vid bestämning av erforderliga säkerhetsnivåer (SIL)

Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels

Som svensk standard gäller europastandarden EN 61511-3:2004. Den svenska standarden innehåller den officiella engelska språkversionen av EN 61511-3:2004.

Nationellt förord

Europastandarden EN 61511-3:2004[*)]

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 61511-3, First edition, 2003 - Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels**

jämte

Corrigendum, October 2004

utarbetad inom International Electrotechnical Commission, IEC.

[*)] EN 61511-3:2004 ikraftsattes 2005-09-26 som SS-EN 61511-3 genom offentliggörande, d v s utan utgivning av något svenskt dokument.

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 61511-3**

NORME EUROPÉENNE

EUROPÄISCHE NORM December 2004

ICS 25.040.01

English version

Functional safety – Safety instrumented systems for the process industry sector Part 3: Guidance for the determination of the required safety integrity levels

(IEC 61511-3:2003 + corrigendum 2004)

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation Partie 3: Conseils pour la détermination des niveaux d'intégrité de sécurité (CEI 61511-3:2003)

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2003 + Corrigendum 2004)

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 61511-3:2004 E

SEK Svensk Elstandard

Foreword

The text of the International Standard IEC 61511-3:2003, 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 61511-3 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

Endorsement notice

The text of the International Standard IEC 61511-3:2003 + corrigendum October 2004 was approved by CENELEC as a European Standard without any modification.

IEC 61511-3
(First edition – 2003)

Functional safety – Safety instrumented systems for the process industry sector

Part 3: Guidance for the determination of the required safety integrity levels

CORRIGENDUM 1

Page 37

Table D.2 – Example calibration of the general purpose risk graph

"Comments" column, on page 38, comment 6:

Instead of: "D is a calibration factor…"

Read: "C is a calibration factor…."

Pages 48 and 49

Reverse the order of Table F.4 and Table F.3. In Clause F.6, second sentence, change the reference to Table F.4 to Table F.3 and in Clause F.7, last sentence, change the reference to Table F.3 to Table F.4.

Page 50

F.10 Intermediate event likelihood

Last paragraph, penultimate sentence:

Instead of: "…Figure 1…"

Read: "…Figure F.1…"

Page 52

F.14.9 Intermediate event likelihood, *first sentence:*

F.14.10 SIS, *last sentence:*

F.14.11 Next SIF, *second sentence:*

Instead of: "…Figure 1…"

Read: "…Figure F.1…"

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 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 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 (E)/Electronic (E)/Programmable Electronic (PE) 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 of IEC 61511-1).

This standard sets out an approach for safety lifecycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy be 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). Any safety strategy should consider each individual safety instrumented system in the context of the other protective systems. 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 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.

This standard deals with guidance in the area of determining the required SIL in hazards and risk analysis (H & RA). The information herein is intended to provide a broad overview of the wide range of global methods used to implement H & RA. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of safety integrity level(s) (SIL) provided in IEC 61511-1 should be reviewed. The annexes in this standard address the following:

Annex A provides an overview of the concepts of tolerable risk and ALARP.

Annex B provides an overview of a semi-quantitative method used to determine the required SIL.

Annex C provides an overview of a safety matrix method to determine the required SIL.

Annex D provides an overview of a method using a semi-qualitative risk graph approach to determine the required SIL.

Annex E provides an overview of a method using a qualitative risk graph approach to determine the required SIL.

Annex F provides an overview of a method using a layer of protection analysis (LOPA) approach to select the required SIL.

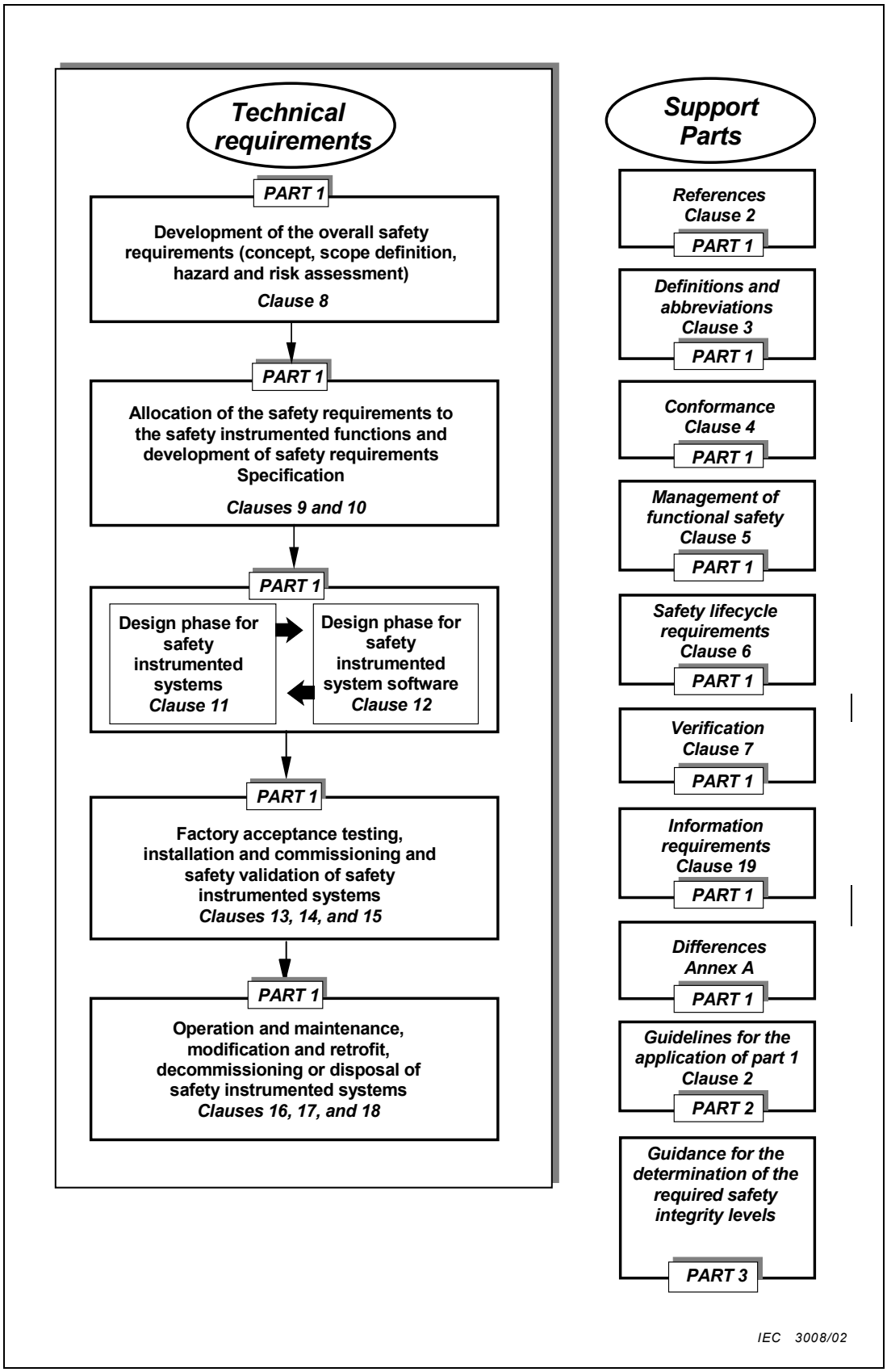

Figure 1 – Overall framework of this standard

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

Part 3: Guidance for the determination of the required safety integrity levels

1 Scope

This part of IEC 61511 provides information on

– the underlying concepts of risk, the relationship of risk to safety integrity, see Clause 3;
– the determination of tolerable risk, see Annex A;
– a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined, see Annexes B, C, D, E, and F.

In particular, this part

a) applies when functional safety is achieved using one or more safety instrumented functions for the protection of either personnel, the general public, or the environment;
b) may be applied in non-safety applications such as asset protection;
c) illustrates typical hazard and risk assessment methods that may be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;
d) illustrates techniques/measures available for determining the required safety integrity levels;
e) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications;
f) does not give examples of determining the requirements for other methods of risk reduction.

Annexes B, C, D, E, and F illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account.

NOTE Those intending to apply the methods indicated in these annexes should consult the source material referenced in each annex.

Figure 1 shows the overall framework for IEC 61511-1, IEC 61511-2 and IEC 61511-3 and indicates the role that this standard plays in the achievement of functional safety for safety instrumented systems.

Figure 2 gives an overview of risk reduction methods.

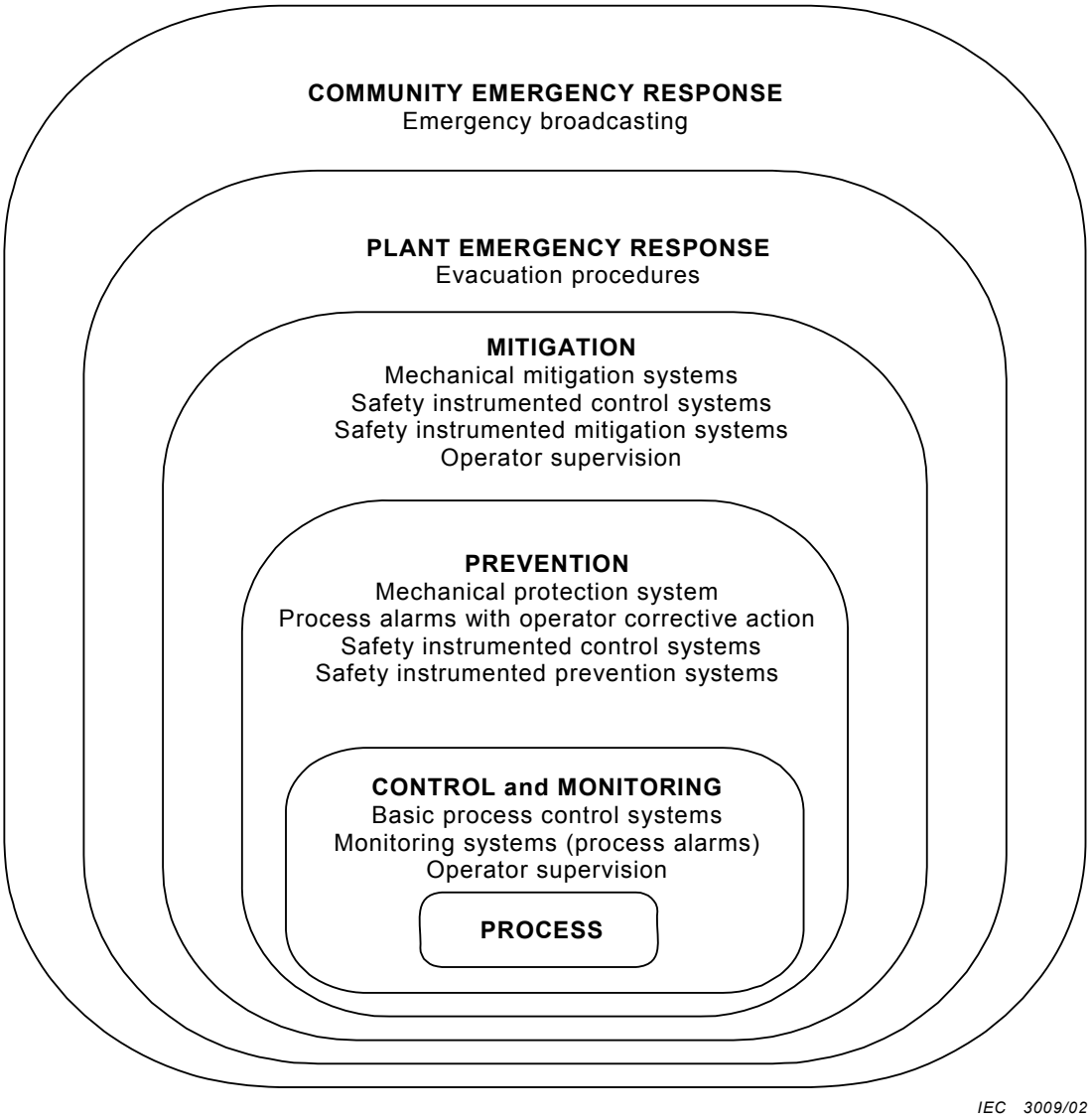

Figure 2 – Typical risk reduction methods found in process plants (for example, protection layer model)