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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 61511-3:2017 sisaldab Euroopa standardi EN 61511-3:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 61511-3:2017 consists of the English text of the European standard EN 61511-3:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 21.04.2017.	Date of Availability of the European standard is 21.04.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 13.110, 25.040.01

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61511-3

April 2017

ICS 13.110; 25.040.01

Supersedes EN 61511-3:2004

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 61511-3:2016)

Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation - Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité (IEC 61511-3:2016)

Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie - Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2016)

This European Standard was approved by CENELEC on 2016-08-25. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre has the same status as the official versions.

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

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

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

European foreword

The text of document 65A/779/FDIS, future edition 2 of IEC 61511-3, prepared by SC 65A “System aspects” of IEC/TC 65 “Industrial process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61511-3:2017.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2017-10-21
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2020-04-21

This document supersedes EN 61511-3:2004.

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

Endorsement notice

The text of the International Standard IEC 61511-3:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61025:2006	NOTE	Harmonized as EN 61025:2007.
IEC 61165:2006	NOTE	Harmonized as EN 61165:2006.
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010.
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010.
IEC 62551:2012	NOTE	Harmonized as EN 62551:2012.
ISO/TR 12489:2013	NOTE	Harmonized as CEN ISO/TR 12489:2016.

Annex ZA
(normative)
Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 61511-1	2016	Functional safety - Safety instrumented systems for the process industry sector - Normative (uon) -- Part 1: Framework, definitions, system, hardware and software requirements	EN 61511-1	2016

CONTENTS

INTRODUCTION

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

The IEC 61511 series addresses the application of SIS for the process industries. A process hazard and risk assessment is carried out to enable the specification for SIS 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 SIS. The SIS includes all devices and subsystems necessary to carry out the SIF from sensor(s) to final element(s).

The IEC 61511 series has two concepts which are fundamental to its application; SIS safety life-cycle and safety integrity levels (SIL).

The IEC 61511 series addresses SIS 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 the IEC 61511 series should be applied. The IEC 61511 series also addresses the SIS sensors and final elements regardless of the technology used. The IEC 61511 series is process industry specific within the framework of IEC 61508:2010.

The IEC 61511 series sets out an approach for SIS 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, and programmable electronic). Any safety strategy should consider each individual SIS in the context of the other protective systems. To facilitate this approach, the IEC 61511 series covers:

– a hazard and risk assessment is carried out to identify the overall safety requirements;
– an allocation of the safety requirements to the SIS is carried out;
– works within a framework which is applicable to all instrumented means 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;
– addressing all SIS safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
– enabling existing or new country specific process industry standards to be harmonized with the IEC 61511 series.

The IEC 61511 series 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 regulations, these take precedence over the requirements defined in the IEC 61511-1.

The IEC 61511-3 deals with guidance in the area of determining the required SIL in hazards and risk assessment. The information herein is intended to provide a broad overview of the wide range of global methods used to implement hazards and risk assessment. The information provided is not of sufficient detail to implement any of these approaches.

Before proceeding, the concept and determination of SIL provided in IEC 61511-1:2016should be reviewed. The informative annexes in the IEC 61511-3 address the following:

Annex A provides information that is common to each of the hazard and risk assessment methods shown herein.

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.

Annex G provides a layer of protection analysis using a risk matrix.

Annex H provides an overview of a qualitative approach for risk estimation & SIL assignment.

Annex I provides an overview of the basic steps involved in designing and calibrating a risk graph.

Annex J provides an overview of the impact of multiple safety systems on determining the required SIL

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

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

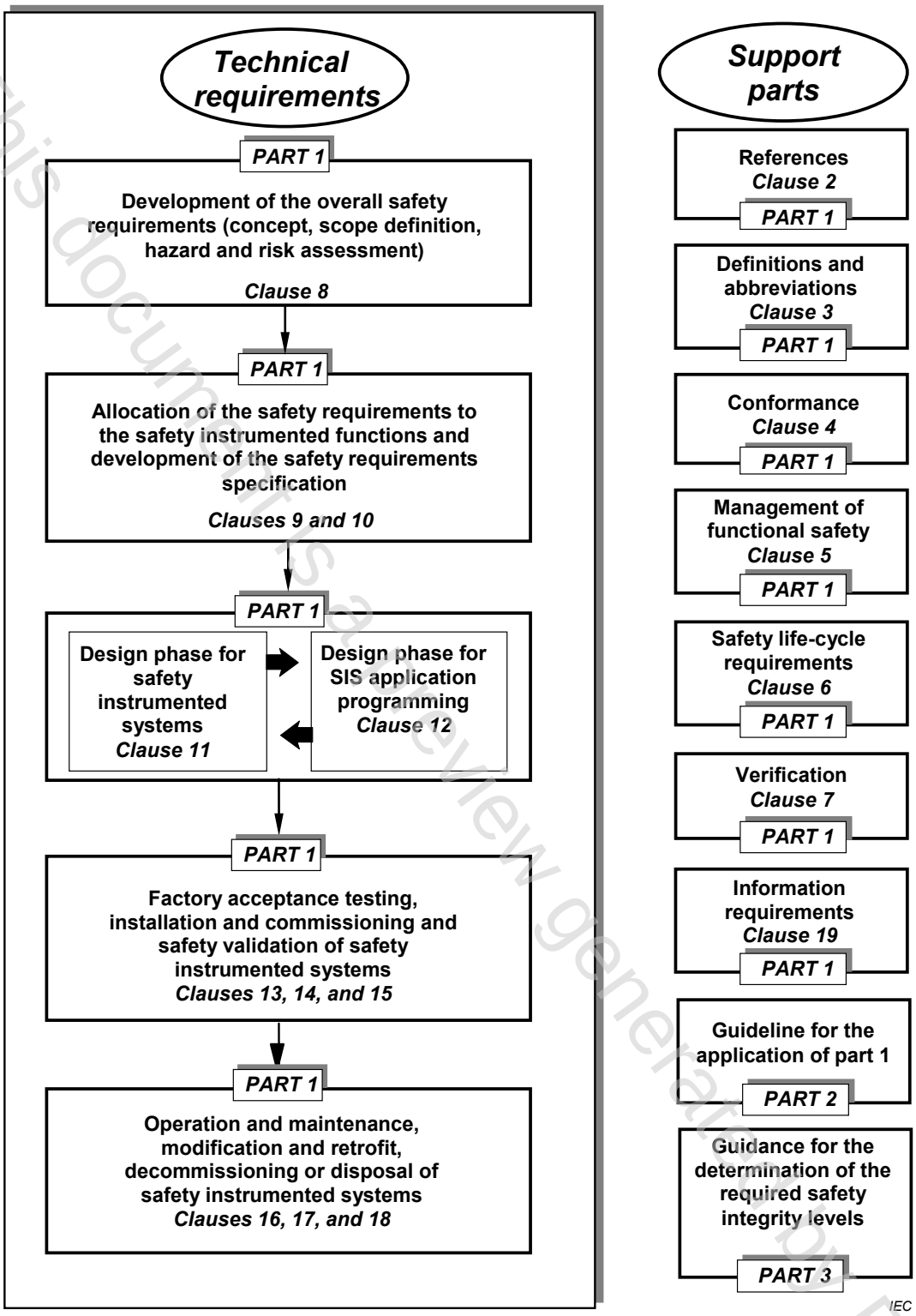

Figure 1 – Overall framework of the IEC 61511 series

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 and the relationship of risk to safety integrity (see Clause A.4);

– the determination of tolerable risk (see Annex K);

– a number of different methods that enable the safety integrity level (SIL) for the safety instrumented functions (SIF) to be determined (see Annexes B through K);

– the impact of multiple safety systems on calculations determining the ability to achieve the desired risk reduction (see Annex J).

In particular, this part of IEC 61511:

a) applies when functional safety is achieved using one or more SIF 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 SIL of each SIF;

d) illustrates techniques/measures available for determining the required SIL;

e) provides a framework for establishing SIL but does not specify the SIL required for specific applications;

f) does not give examples of determining the requirements for other methods of risk reduction.

NOTE Examples given in the Annexes of this Standard are intended only as case specific examples of implementing IEC 61511 requirements in a specific instance, and the user should satisfy themselves that the chosen methods and techniques are appropriate to their situation.

Annexes B through K 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 1 Those intending to apply the methods indicated in these annexes can consult the source material referenced in each annex.

NOTE 2 The methods of SIL determination included in Part 3 may not be suitable for all applications. In particular, specific techniques or additional factors that are not illustrated may be required for high demand or continuous mode of operation.

NOTE 3 The methods as illustrated herein may result in non-conservative results when they are used beyond their underlying limits and when factors such as common cause, fault tolerance, holistic considerations of the application, lack of experience with the method being used, independence of the protection layers, etc., are not properly considered. See Annex J.

Figure 2 gives an overview of typical protection layers and risk reduction means.