

# SLOVENSKI STANDARD

## SIST EN IEC 62061:2021

01-oktober-2021

Nadomešča:

SIST EN 62061:2005

SIST EN 62061:2005/A1:2013

SIST EN 62061:2005/A2:2016

---

**Varnost strojev - Funkcijska varnost nadzornih sistemov, povezanih z varnostjo (IEC 62061:2021)**

Safety of machinery - Functional safety of safety-related control systems (IEC 62061:2021)

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)

Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (IEC 62061:2021)

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

Sécurité des machines - Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité (IEC 62061:2021)

**Ta slovenski standard je istoveten z: EN IEC 62061:2021**

---

**ICS:**

|           |                                                |                                            |
|-----------|------------------------------------------------|--------------------------------------------|
| 13.110    | Varnost strojev                                | Safety of machinery                        |
| 25.040.40 | Merjenje in krmiljenje industrijskih postopkov | Industrial process measurement and control |

**SIST EN IEC 62061:2021**

**en,fr,de**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN IEC 62061:2021](https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021)

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**EN IEC 62061**

July 2021

ICS 13.110; 25.040.99; 29.020

Supersedes EN 62061:2005 and all of its amendments  
and corrigenda (if any)

English Version

**Safety of machinery - Functional safety of safety-related control  
systems  
(IEC 62061:2021)**

Sécurité des machines - Sécurité fonctionnelle des  
systèmes de commande relatifs à la sécurité  
(IEC 62061:2021)

Sicherheit von Maschinen - Funktionale Sicherheit  
sicherheitsbezogener Steuerungssysteme  
(IEC 62061:2021)

This European Standard was approved by CENELEC on 2021-04-26. 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.

SIST EN IEC 62061:2021

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, 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: Rue de la Science 23, B-1040 Brussels**

**EN IEC 62061:2021 (E)****European foreword**

The text of document 44/885/FDIS, future edition 2 of IEC 62061, prepared by IEC/TC 44 "Safety of machinery - Electrotechnical aspects" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62061:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2022-01-26 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2024-04-26 document have to be withdrawn

This document supersedes EN 62061:2005 and all of its amendments and corrigenda (if any).

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

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

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

**iTeh STANDARD PREVIEW**

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

**Endorsement notice**

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

The text of the International Standard IEC 62061:2021 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 60068 (series)  | NOTE | Harmonized as EN 60068 (series)                              |
| IEC 60364-4-41:2005 | NOTE | Harmonized as HD 60364-4-41:2017                             |
| IEC 60529           | NOTE | Harmonized as EN 60529                                       |
| IEC 60721 (series)  | NOTE | Harmonized as EN 60721-3-9:1993/A1 (series)                  |
| IEC 60812           | NOTE | Harmonized as EN IEC 60812                                   |
| IEC 60947-4-1:2018  | NOTE | Harmonized as EN IEC 60947-4-1:2019 (not modified)           |
| IEC 60947-5-1       | NOTE | Harmonized as EN 60947-5-1                                   |
| IEC 60947-5-3       | NOTE | Harmonized as EN 60947-5-3                                   |
| IEC 60947-5-5       | NOTE | Harmonized as EN 60947-5-5                                   |
| IEC 60947-5-8       | NOTE | Harmonized as EN IEC 60947-5-8                               |
| IEC 61000-6-7       | NOTE | Harmonized as EN 61000-6-7                                   |
| IEC 61025:2006      | NOTE | Harmonized as EN 61025:2007 (not modified)                   |
| IEC 61131-2:2017    | NOTE | Harmonized as EN 61131-2:2017 (not modified) to be published |
| IEC 61131-6:2012    | NOTE | Harmonized as EN 61131-6:2012 (not modified)                 |

|                          |      |                                                      |
|--------------------------|------|------------------------------------------------------|
| IEC 61140:2016           | NOTE | Harmonized as EN 61140:2016 (not modified)           |
| IEC 61165                | NOTE | Harmonized as EN 61165                               |
| IEC 61204-7:2016         | NOTE | Harmonized as EN IEC 61204-7:2018 (not modified)     |
| IEC 61310 (series)       | NOTE | Harmonized as EN 61310 (series)                      |
| IEC 61326-3-1            | NOTE | Harmonized as EN 61326-3-1                           |
| IEC 61496 (series)       | NOTE | Harmonized as EN IEC 61496 (series)                  |
| IEC 61508-1:2010         | NOTE | Harmonized as EN 61508-1:2010 (not modified)         |
| IEC 61508-4:2010         | NOTE | Harmonized as EN 61508-4:2010 (not modified)         |
| IEC 61508-5:2010         | NOTE | Harmonized as EN 61508-5:2010 (not modified)         |
| IEC 61508-6:2010         | NOTE | Harmonized as EN 61508-6:2010 (not modified)         |
| IEC 61508-7:2010         | NOTE | Harmonized as EN 61508-7:2010 (not modified)         |
| IEC 61511 (series)       | NOTE | Harmonized as EN 61511 (series)                      |
| IEC 61511-1:2016         | NOTE | Harmonized as EN 61511-1:2017 (not modified)         |
| IEC 61511-1:2016/A1:2017 | NOTE | Harmonized as EN 61511-1:2017/A1:2017 (not modified) |
| IEC 61511-3:2016         | NOTE | Harmonized as EN 61511-3:2017 (not modified)         |
| IEC 61649                | NOTE | Harmonized as EN 61649                               |
| IEC 61709:2017           | NOTE | Harmonized as EN 61709:2017 (not modified)           |
| IEC 61784-3 (series)     | NOTE | Harmonized as EN 61784-3 (series)                    |
| IEC 61784-3:2016         | NOTE | Harmonized as EN 61784-3:2016 (not modified)         |
| IEC 61800-5-2            | NOTE | Harmonized as EN 61800-5-2                           |
| IEC 61810 (series)       | NOTE | Harmonized as EN 61810 (series)                      |
| IEC 62443 (series)       | NOTE | Harmonized as EN IEC 62443 (series)                  |
| IEC 62477 (series)       | NOTE | Harmonized as EN IEC 62477 (series)                  |
| IEC 62502                | NOTE | Harmonized as EN 62502                               |
| ISO/IEC 27001:2013       | NOTE | Harmonized as EN ISO/IEC 27001:2017 (not modified)   |
| ISO 4413:2010            | NOTE | Harmonized as EN ISO 4413:2010 (not modified)        |
| ISO 4414:2010            | NOTE | Harmonized as EN ISO 4414:2010 (not modified)        |
| ISO 11161:2007           | NOTE | Harmonized as EN ISO 11161:2007 (not modified)       |
| ISO 13850:2015           | NOTE | Harmonized as EN ISO 13850:2015 (not modified)       |
| ISO 13851:2019           | NOTE | Harmonized as EN ISO 13851:2019 (not modified)       |
| ISO 13855:2010           | NOTE | Harmonized as EN ISO 13855:2010 (not modified)       |
| ISO 14118:2017           | NOTE | Harmonized as EN ISO 14118:2018 (not modified)       |
| ISO 14119:2013           | NOTE | Harmonized as EN ISO 14119:2013 (not modified)       |
| ISO/TR 22100-4:2018      | NOTE | Harmonized as CEN ISO/TR 22100-4:2020 (not modified) |

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/29d65a08-4596-4586-86b8-37924b05e39b/sist-en-iec-62061-2021>

## Annex ZA

### (normative)

### Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 1 Where 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](http://www.cenelec.eu).

| <u>Publication</u> | <u>Year</u> | <u>Title</u>                                                                                                                                                                                                     | <u>EN/HD</u>   | <u>Year</u> |
|--------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------|
| IEC 60204-1 (mod)  | 2016        | Safety of machinery - Electrical equipment of machines - Part 1: General requirements                                                                                                                            | EN 60204-1     | 2018        |
| IEC 61000-1-2      | 2016        | Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena | EN 61000-1-2   | 2016        |
| IEC 61508          | series      | Functional safety of electrical/electronic/programmable electronic safety-related systems                                                                                                                        | EN 61508       | series      |
| IEC 61508-2        | 2010        | Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems                        | EN 61508-2     | 2010        |
| IEC 61508-3        | 2010        | Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements                                                                                        | EN 61508-3     | 2010        |
| ISO 12100          | 2010        | Safety of machinery - General principles for design - Risk assessment and risk reduction                                                                                                                         | EN ISO 12100   | 2010        |
| ISO 13849          | series      | Safety of machinery - Safety-related parts of control systems                                                                                                                                                    | EN ISO 13849   | series      |
| ISO 13849-1        | 2015        | Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design                                                                                                            | EN ISO 13849-1 | 2015        |
| ISO 13849-2        | 2012        | Safety of machinery - Safety-related parts of control systems - Part 2: Validation                                                                                                                               | EN ISO 13849-2 | 2012        |

## Annex ZZ (informative)

### Relationship between this European standard and the essential requirements of Directive 2006/42/EC [2006 OJ L 157] aimed to be covered

This European standard has been prepared under a Commission's standardisation request "M/396" to provide one voluntary means of conforming to *essential* requirements of Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) [2006 OJ L 157].

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZZ.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive, and associated EFTA regulations.

**Table ZZ.1 — Correspondence between this European standard and Annex 1 of Directive] 2006/42/EC [2006 OJ L 157]**

| The relevant Essential Requirements of Directive 2006/42/EC | Clause(s) / sub-clause(s) of this EN | Remarks / Notes                                                     |
|-------------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------|
| 1.2.1                                                       | Clauses 4, 5, 6, 7, 8, 9.            |                                                                     |
| 1.7.4.2 (e, g, i, r, s)                                     | 10.3<br><br>SIST EN IEC 62061:2021   | This subclause only deals with the instruction for safety functions |

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

**WARNING 1:** Presumption of conformity stays valid only as long as a reference to this European standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

**WARNING 2:** Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN IEC 62061:2021](https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021)

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>





IEC 62061

Edition 2.0 2021-03

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**Safety of machinery – Functional safety of safety-related control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande  
relatifs à la sécurité**

SIST EN IEC 62061:2021

<https://standards.iteh.ai/catalog/standards/sist/29d83a08-a396-4586-86b8-3d924b05c39b/sist-en-iec-62061-2021>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-9333-1

**Warning! Make sure that you obtained this publication from an authorized distributor.**  
**Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## CONTENTS

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| FOREWORD.....                                                              | 8  |
| INTRODUCTION.....                                                          | 10 |
| 1 Scope.....                                                               | 11 |
| 2 Normative references .....                                               | 12 |
| 3 Terms, definitions and abbreviations .....                               | 13 |
| 3.1 Alphabetical list of definitions.....                                  | 13 |
| 3.2 Terms and definitions.....                                             | 15 |
| 3.3 Abbreviations.....                                                     | 28 |
| 4 Design process of an SCS and management of functional safety.....        | 28 |
| 4.1 Objective .....                                                        | 28 |
| 4.2 Design process .....                                                   | 29 |
| 4.3 Management of functional safety using a functional safety plan .....   | 31 |
| 4.4 Configuration management .....                                         | 33 |
| 4.5 Modification .....                                                     | 33 |
| 5 Specification of a safety function .....                                 | 34 |
| 5.1 Objective .....                                                        | 34 |
| 5.2 Safety requirements specification (SRS).....                           | 34 |
| 5.2.1 General.....                                                         | 34 |
| 5.2.2 Information to be available.....                                     | 34 |
| 5.2.3 Functional requirements specification.....                           | 35 |
| 5.2.4 Estimation of demand mode of operation .....                         | 35 |
| 5.2.5 Safety integrity requirements specification.....                     | 36 |
| 6 Design of an SCS.....                                                    | 37 |
| 6.1 General.....                                                           | 37 |
| 6.2 Subsystem architecture based on top down decomposition .....           | 37 |
| 6.3 Basic methodology – Use of subsystem .....                             | 37 |
| 6.3.1 General .....                                                        | 37 |
| 6.3.2 SCS decomposition .....                                              | 38 |
| 6.3.3 Sub-function allocation .....                                        | 39 |
| 6.3.4 Use of a pre-designed subsystem.....                                 | 39 |
| 6.4 Determination of safety integrity of the SCS.....                      | 40 |
| 6.4.1 General .....                                                        | 40 |
| 6.4.2 PFH.....                                                             | 40 |
| 6.5 Requirements for systematic safety integrity of the SCS .....          | 41 |
| 6.5.1 Requirements for the avoidance of systematic hardware failures ..... | 41 |
| 6.5.2 Requirements for the control of systematic faults.....               | 42 |
| 6.6 Electromagnetic immunity .....                                         | 43 |
| 6.7 Software based manual parameterization.....                            | 43 |
| 6.7.1 General .....                                                        | 43 |
| 6.7.2 Influences on safety-related parameters .....                        | 43 |
| 6.7.3 Requirements for software based manual parameterization .....        | 44 |
| 6.7.4 Verification of the parameterization tool.....                       | 45 |
| 6.7.5 Performance of software based manual parameterization .....          | 45 |
| 6.8 Security aspects .....                                                 | 45 |
| 6.9 Aspects of periodic testing .....                                      | 46 |
| 7 Design and development of a subsystem.....                               | 46 |

|        |                                                                                       |    |
|--------|---------------------------------------------------------------------------------------|----|
| 7.1    | General.....                                                                          | 46 |
| 7.2    | Subsystem architecture design .....                                                   | 47 |
| 7.3    | Requirements for the selection and design of subsystem and subsystem elements .....   | 48 |
| 7.3.1  | General .....                                                                         | 48 |
| 7.3.2  | Systematic integrity .....                                                            | 48 |
| 7.3.3  | Fault consideration and fault exclusion .....                                         | 51 |
| 7.3.4  | Failure rate of subsystem element .....                                               | 52 |
| 7.4    | Architectural constraints of a subsystem .....                                        | 55 |
| 7.4.1  | General .....                                                                         | 55 |
| 7.4.2  | Estimation of safe failure fraction ( <i>SFF</i> ) .....                              | 56 |
| 7.4.3  | Behaviour (of the SCS) on detection of a fault in a subsystem .....                   | 57 |
| 7.4.4  | Realization of diagnostic functions .....                                             | 58 |
| 7.5    | Subsystem design architectures .....                                                  | 59 |
| 7.5.1  | General .....                                                                         | 59 |
| 7.5.2  | Basic subsystem architectures .....                                                   | 59 |
| 7.5.3  | Basic requirements .....                                                              | 61 |
| 7.6    | <i>PFH</i> of subsystems .....                                                        | 62 |
| 7.6.1  | General .....                                                                         | 62 |
| 7.6.2  | Methods to estimate the <i>PFH</i> of a subsystem .....                               | 62 |
| 7.6.3  | Simplified approach to estimation of contribution of common cause failure (CCF) ..... | 62 |
| 8      | Software .....                                                                        | 62 |
| 8.1    | General.....                                                                          | 62 |
| 8.2    | Definition of software levels .....                                                   | 63 |
| 8.3    | Software – Level 1 .....                                                              | 64 |
| 8.3.1  | Software safety lifecycle – SW level 1 .....                                          | 64 |
| 8.3.2  | Software design – SW level 1 .....                                                    | 65 |
| 8.3.3  | Module design – SW level 1 .....                                                      | 67 |
| 8.3.4  | Coding – SW level 1 .....                                                             | 67 |
| 8.3.5  | Module test – SW level 1 .....                                                        | 68 |
| 8.3.6  | Software testing – SW level 1 .....                                                   | 68 |
| 8.3.7  | Documentation – SW level 1 .....                                                      | 69 |
| 8.3.8  | Configuration and modification management process – SW level 1 .....                  | 69 |
| 8.4    | Software level 2 .....                                                                | 70 |
| 8.4.1  | Software safety lifecycle – SW level 2 .....                                          | 70 |
| 8.4.2  | Software design – SW level 2 .....                                                    | 71 |
| 8.4.3  | Software system design – SW level 2 .....                                             | 73 |
| 8.4.4  | Module design – SW level 2 .....                                                      | 73 |
| 8.4.5  | Coding – SW level 2 .....                                                             | 74 |
| 8.4.6  | Module test – SW level 2 .....                                                        | 75 |
| 8.4.7  | Software integration testing SW level 2 .....                                         | 75 |
| 8.4.8  | Software testing SW level 2 .....                                                     | 75 |
| 8.4.9  | Documentation – SW level 2 .....                                                      | 76 |
| 8.4.10 | Configuration and modification management process – SW level 2 .....                  | 77 |
| 9      | Validation .....                                                                      | 77 |
| 9.1    | Validation principles .....                                                           | 77 |
| 9.1.1  | Validation plan .....                                                                 | 80 |
| 9.1.2  | Use of generic fault lists .....                                                      | 80 |

|                       |                                                                   |     |
|-----------------------|-------------------------------------------------------------------|-----|
| 9.1.3                 | Specific fault lists .....                                        | 80  |
| 9.1.4                 | Information for validation .....                                  | 81  |
| 9.1.5                 | Validation record .....                                           | 81  |
| 9.2                   | Analysis as part of validation .....                              | 82  |
| 9.2.1                 | General .....                                                     | 82  |
| 9.2.2                 | Analysis techniques .....                                         | 82  |
| 9.2.3                 | Verification of safety requirements specification (SRS) .....     | 82  |
| 9.3                   | Testing as part of validation .....                               | 83  |
| 9.3.1                 | General .....                                                     | 83  |
| 9.3.2                 | Measurement accuracy .....                                        | 83  |
| 9.3.3                 | More stringent requirements .....                                 | 84  |
| 9.3.4                 | Test samples .....                                                | 84  |
| 9.4                   | Validation of the safety function .....                           | 84  |
| 9.4.1                 | General .....                                                     | 84  |
| 9.4.2                 | Analysis and testing .....                                        | 85  |
| 9.5                   | Validation of the safety integrity of the SCS .....               | 85  |
| 9.5.1                 | General .....                                                     | 85  |
| 9.5.2                 | Validation of subsystem(s) .....                                  | 85  |
| 9.5.3                 | Validation of measures against systematic failures .....          | 86  |
| 9.5.4                 | Validation of safety-related software .....                       | 86  |
| 9.5.5                 | Validation of combination of subsystems .....                     | 87  |
| 10                    | Documentation .....                                               | 87  |
| 10.1                  | General .....                                                     | 87  |
| 10.2                  | Technical documentation .....                                     | 87  |
| 10.3                  | Information for use of the SCS .....                              | 89  |
| 10.3.1                | General .....                                                     | 89  |
| 10.3.2                | Information for use given by the manufacturer of subsystems ..... | 89  |
| 10.3.3                | Information for use given by the SCS integrator .....             | 90  |
| Annex A (informative) | Determination of required safety integrity .....                  | 92  |
| A.1                   | General .....                                                     | 92  |
| A.2                   | Matrix assignment for the required SIL .....                      | 92  |
| A.2.1                 | Hazard identification/indication .....                            | 92  |
| A.2.2                 | Risk estimation .....                                             | 92  |
| A.2.3                 | Severity (Se) .....                                               | 93  |
| A.2.4                 | Probability of occurrence of harm .....                           | 93  |
| A.2.5                 | Class of probability of harm (CI) .....                           | 96  |
| A.2.6                 | SIL assignment .....                                              | 96  |
| A.3                   | Overlapping hazards .....                                         | 98  |
| Annex B (informative) | Example of SCS design methodology .....                           | 99  |
| B.1                   | General .....                                                     | 99  |
| B.2                   | Safety requirements specification .....                           | 99  |
| B.3                   | Decomposition of the safety function .....                        | 99  |
| B.4                   | Design of the SCS by using subsystems .....                       | 100 |
| B.4.1                 | General .....                                                     | 100 |
| B.4.2                 | Subsystem 1 design – “guard door monitoring” .....                | 100 |
| B.4.3                 | Subsystem 2 design – “evaluation logic” .....                     | 102 |
| B.4.4                 | Subsystem 3 design – “motor control” .....                        | 103 |
| B.4.5                 | Evaluation of the SCS .....                                       | 103 |
| B.4.6                 | PFH .....                                                         | 104 |

|              |                                                                                                    |     |
|--------------|----------------------------------------------------------------------------------------------------|-----|
| B.5          | Verification.....                                                                                  | 104 |
| B.5.1        | General .....                                                                                      | 104 |
| B.5.2        | Analysis.....                                                                                      | 104 |
| B.5.3        | Tests .....                                                                                        | 105 |
| Annex C      | (informative) Examples of $MTTF_D$ values for single components .....                              | 106 |
| C.1          | General.....                                                                                       | 106 |
| C.2          | Good engineering practices method .....                                                            | 106 |
| C.3          | Hydraulic components.....                                                                          | 106 |
| C.4          | $MTTF_D$ of pneumatic, mechanical and electromechanical components .....                           | 107 |
| Annex D      | (informative) Examples for diagnostic coverage ( $DC$ ).....                                       | 109 |
| Annex E      | (informative) Methodology for the estimation of susceptibility to common cause failures (CCF)..... | 111 |
| E.1          | General.....                                                                                       | 111 |
| E.2          | Methodology .....                                                                                  | 111 |
| E.2.1        | Requirements for CCF .....                                                                         | 111 |
| E.2.2        | Estimation of effect of CCF .....                                                                  | 111 |
| Annex F      | (informative) Guideline for software level 1 .....                                                 | 114 |
| F.1          | Software safety requirements.....                                                                  | 114 |
| F.2          | Coding guidelines .....                                                                            | 115 |
| F.3          | Specification of safety functions.....                                                             | 116 |
| F.4          | Specification of hardware design .....                                                             | 117 |
| F.5          | Software system design specification.....                                                          | 119 |
| F.6          | Protocols .....                                                                                    | 121 |
| Annex G      | (informative) Examples of safety functions.....                                                    | 124 |
| Annex H      | (informative) Simplified approaches to evaluate the $PFH$ value of a subsystem .....               | 125 |
| H.1          | Table allocation approach .....                                                                    | 125 |
| H.2          | Simplified formulas for the estimation of $PFH$ .....                                              | 127 |
| H.2.1        | General .....                                                                                      | 127 |
| H.2.2        | Basic subsystem architecture A: single channel without a diagnostic function .....                 | 127 |
| H.2.3        | Basic subsystem architecture B: dual channel without a diagnostic function .....                   | 128 |
| H.2.4        | Basic subsystem architecture C: single channel with a diagnostic function .....                    | 128 |
| H.2.5        | Basic subsystem architecture D: dual channel with a diagnostic function(s) .....                   | 133 |
| H.3          | Parts count method.....                                                                            | 134 |
| Annex I      | (informative) The functional safety plan and design activities .....                               | 135 |
| I.1          | General.....                                                                                       | 135 |
| I.2          | Example of a machine design plan including a safety plan .....                                     | 135 |
| I.3          | Example of activities, documents and roles .....                                                   | 135 |
| Annex J      | (informative) Independence for reviews and testing/verification/validation activities .....        | 138 |
| J.1          | Software design .....                                                                              | 138 |
| J.2          | Validation.....                                                                                    | 138 |
| Bibliography | .....                                                                                              | 140 |
| Figure 1     | – Scope of this document.....                                                                      | 12  |

|                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 2 – Integration within the risk reduction process of ISO 12100 (extract) .....                                       | 29  |
| Figure 3 – Iterative process for design of the safety-related control system .....                                          | 30  |
| Figure 4 – Example of a combination of subsystems as one SCS.....                                                           | 31  |
| Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand .....      | 36  |
| Figure 6 – Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems ..... | 39  |
| Figure 7 – Example of safety integrity of a safety function based on allocated subsystems as one SCS .....                  | 40  |
| Figure 8 – Subsystem A logical representation .....                                                                         | 60  |
| Figure 9 – Subsystem B logical representation .....                                                                         | 60  |
| Figure 10 – Subsystem C logical representation .....                                                                        | 60  |
| Figure 11 – Subsystem D logical representation .....                                                                        | 61  |
| Figure 12 – V-model for SW level 1.....                                                                                     | 64  |
| Figure 13 – V-model for software modules customized by the designer for SW level 1 .....                                    | 64  |
| Figure 14 – V-model of software safety lifecycle for SW level 2.....                                                        | 70  |
| Figure 15 – Overview of the validation process .....                                                                        | 79  |
| Figure A.1 – Parameters used in risk estimation .....                                                                       | 92  |
| Figure A.2 – Example proforma for SIL assignment process .....                                                              | 98  |
| Figure B.1 – Decomposition of the safety function.....                                                                      | 100 |
| Figure B.2 – Overview of design of the subsystems of the SCS .....                                                          | 100 |
| Figure F.1 – Plant sketch .....                                                                                             | 116 |
| Figure F.2 – Principal module architecture design.....                                                                      | 119 |
| Figure F.3 – Principal design approach of logical evaluation.....                                                           | 120 |
| Figure F.4 – Example of logical representation (program sketch) .....                                                       | 121 |
| Figure H.1 – Subsystem A logical representation .....                                                                       | 127 |
| Figure H.2 – Subsystem B logical representation .....                                                                       | 128 |
| Figure H.3 – Subsystem C logical representation .....                                                                       | 128 |
| Figure H.4 – Correlation of subsystem C and the pertinent fault handling function .....                                     | 129 |
| Figure H.5 – Subsystem C with external fault handling function .....                                                        | 129 |
| Figure H.6 – Subsystem C with external fault diagnostics .....                                                              | 131 |
| Figure H.7 – Subsystem C with external fault reaction .....                                                                 | 131 |
| Figure H.8 – Subsystem C with internal fault diagnostics and internal fault reaction.....                                   | 131 |
| Figure H.9 – Subsystem D logical representation .....                                                                       | 133 |
| Figure I.1 – Example of a machine design plan including a safety plan .....                                                 | 135 |
| Figure I.2 – Example of activities, documents and roles .....                                                               | 136 |
| Table 1 – Terms used in IEC 62061 .....                                                                                     | 13  |
| Table 2 – Abbreviations used in IEC 62061.....                                                                              | 28  |
| Table 3 – SIL and limits of <i>PFH</i> values.....                                                                          | 36  |
| Table 4 – Required SIL and <i>PFH</i> of pre-designed subsystem .....                                                       | 40  |
| Table 5 – Relevant information for each subsystem .....                                                                     | 47  |
| Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem .....    | 56  |

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| Table 7 – Overview of basic requirements and interrelation to basic subsystem architectures .....                | 61  |
| Table 8 – Different levels of application software .....                                                         | 63  |
| Table 9 – Documentation of an SCS .....                                                                          | 88  |
| Table A.1 – Severity (Se) classification .....                                                                   | 93  |
| Table A.2 – Frequency and duration of exposure (Fr) classification .....                                         | 94  |
| Table A.3 – Probability (Pr) classification .....                                                                | 95  |
| Table A.4 – Probability of avoiding or limiting harm (Av) classification .....                                   | 96  |
| Table A.5 – Parameters used to determine class of probability of harm (Cl) .....                                 | 96  |
| Table A.6 – Matrix assignment for determining the required SIL (or PL <sub>r</sub> ) for a safety function ..... | 97  |
| Table B.1 – Safety requirements specification – example of overview .....                                        | 99  |
| Table B.2 – Systematic integrity – example of overview .....                                                     | 104 |
| Table B.3 – Verification by tests .....                                                                          | 105 |
| Table C.1 – Standards references and $MTTF_D$ or $B_{10D}$ values for components .....                           | 107 |
| Table D.1 – Estimates for diagnostic coverage ( $DC$ ) .....                                                     | 109 |
| Table E.1 – Criteria for estimation of CCF .....                                                                 | 112 |
| Table E.2 – Criteria for estimation of CCF .....                                                                 | 113 |
| Table F.1 – Example of relevant documents related to the simplified V-model .....                                | 114 |
| Table F.2 – Examples of coding guidelines .....                                                                  | 115 |
| Table F.3 – Specified safety functions .....                                                                     | 117 |
| Table F.4 – Relevant list of input and output signals .....                                                      | 118 |
| Table F.5 – Example of simplified cause and effect matrix .....                                                  | 121 |
| Table F.6 – Verification of software system design specification .....                                           | 122 |
| Table F.7 – Software code review .....                                                                           | 122 |
| Table F.8 – Software validation .....                                                                            | 123 |
| Table G.1 – Examples of typical safety functions .....                                                           | 124 |
| Table H.1 – Allocation of $PFH$ value of a subsystem .....                                                       | 126 |
| Table H.2 – Relationship between $B_{10D}$ , operations and $MTTF_D$ .....                                       | 127 |
| Table H.3 – Minimum value of $1/\lambda_D F_H$ for the applicability of $PFH$ equation (H.4) .....               | 132 |
| Table J.1 – Minimum levels of independence for review, testing and verification activities .....                 | 138 |
| Table J.2 – Minimum levels of independence for validation activities .....                                       | 138 |