



SLOVENSKI STANDARD

SIST EN 61131-6:2013

01-februar-2013

Programirljivi krmilniki - 6. del: Funkcionalna varnost (IEC 61131-6:2012)

Programmable controllers - Part 6: Functional safety (IEC 61131-6:2012)

Speicherprogrammierbare Steuerungen - Teil 6: Funktionale Sicherheit (IEC 61131-6:2012)

Automates programmables - Partie 6: Sécurité fonctionnelle (CEI 61131-6:2012)

ITeH STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: EN 61131-6:2012

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f-9327-0aa9519684d8/sist-en-61131-6-2013>

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
35.240.50	Uporabniške rešitve IT v industriji	IT applications in industry

SIST EN 61131-6:2013

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61131-6:2013

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f9327-0aa9519684d8/sist-en-61131-6-2013>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 61131-6

November 2012

ICS 25.040.40; 35.240.50

English version

**Programmable controllers -
Part 6: Functional safety
(IEC 61131-6:2012)**

Automates programmables -
Partie 6: Sécurité fonctionnelle
(CEI 61131-6:2012)

Speicherprogrammierbare Steuerungen –
Teil 6: Funktionale Sicherheit
(IEC 61131-6:2012)

This European Standard was approved by CENELEC on 2012-11-06. 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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65B/831/FDIS, future edition 1 of IEC 61131-6, prepared by SC 65B, "Devices & process analysis", of IEC TC 65, "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61131-6:2012.

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) 2013-08-06
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2015-11-06

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 61131-6:2012 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 60300-3-2:2004	NOTE	Harmonized as EN 60300-3-2:2005 (not modified).
IEC 61000 series	NOTE	Harmonized in EN 61000 series (not modified).
IEC 61025:2006	NOTE	Harmonized as EN 61025:2007 (not modified).
IEC 61069-7:1999	NOTE	Harmonized as EN 61069-7:1999 (not modified).
IEC 61078:2006	NOTE	Harmonized as EN 61078:2006 (not modified).
IEC 61131-3:2003	NOTE	Harmonized as EN 61131-3:2003 (not modified).
IEC 61165:2006	NOTE	Harmonized as EN 61165:2006 (not modified).
IEC 61496-1:2004 + A1:2007	NOTE	Harmonized as EN 61496-1:2004 (modified) + A1:2008 (not modified).
IEC 61496-3:2008	NOTE	Harmonized as CLC/TS 61496-3:2008 (not modified).
IEC 61508 series	NOTE	Harmonized in EN 61508 series (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 61508-7:2010	NOTE	Harmonized as EN 61508-7:2010 (not modified).
IEC 61511-1:2003	NOTE	Harmonized as EN 61511-1:2004 (not modified).
IEC 61511-2:2003	NOTE	Harmonized as EN 61511-2:2004 (not modified).
IEC 61511-3:2003	NOTE	Harmonized as EN 61511-3:2004 (not modified).

IEC 62061:2005	NOTE	Harmonized as EN 62061:2005 (not modified).
IEC 62079:2001	NOTE	Harmonized as EN 62079:2001 (not modified).
CISPR 11:2009	NOTE	Harmonized as EN 55011:2009 (modified).
ISO 8402:1994	NOTE	Harmonized as EN ISO 8402:1995 (not modified).
ISO 9000-3:1997	NOTE	Harmonized as EN ISO 9000-3:1997 (not modified).
ISO 9001:2008	NOTE	Harmonized as EN ISO 9001:2008 (not modified).
ISO 13849-1:2006	NOTE	Harmonized as EN ISO 13849-1:2008 (not modified).
ISO 13849-2:2003	NOTE	Harmonized as EN ISO 13849-2:2003 (not modified).
ISO 14224:2006	NOTE	Harmonized as EN ISO 14224:2006 (not modified).

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

[SIST EN 61131-6:2013](https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f9327-0aa9519684d8/sist-en-61131-6-2013)

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f9327-0aa9519684d8/sist-en-61131-6-2013>

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

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60947-5-1	2003	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices	EN 60947-5-1 + corr. July	2004 2005
IEC/TS 61000-1-2	2008	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	-	-
IEC 61000-4-2	2008	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test	EN 61000-4-2	2009
IEC 61000-4-3	2006	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test	EN 61000-4-3	2006
IEC 61000-4-4	2012	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test	EN 61000-4-4	2012
IEC 61000-4-5 + corr. October	2005 2009	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test	EN 61000-4-5	2006
IEC 61000-4-6	2008	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields	EN 61000-4-6	2009
IEC 61000-4-8	2009	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test	EN 61000-4-8	2010
IEC 61131-1	2003	Programmable controllers - Part 1: General information	EN 61131-1	2003
IEC 61131-2	2007	Programmable controllers - Part 2: Equipment requirements and tests	EN 61131-2	2007
IEC/TR 61131-4	2004	Programmable controllers - Part 4: User guidelines	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61326-3-1 + corr. August	2008 2008	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications	EN 61326-3-1	2008
IEC 61326-3-2	2008	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment	EN 61326-3-2	2008
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010
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
IEC 61508-6	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	EN 61508-6	2010
IEC 61784-3	2010	Industrial communication networks - Profiles – Part 3: Functional safety fieldbuses - General rules and profile definitions	EN 61784-3	2010
IEC 62443	Series	Security for industrial process measurement and control - Network and system security	-	-
IEC Guide 104	2010	The preparation of safety publications and the use of basic safety publications and group safety publications	-	-
ISO/IEC Guide 51	1999	Safety aspects - Guidelines for their inclusion in standards	-	-
EN 50205	2002	Relays with forcibly guided (mechanically linked) contacts	-	-

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61131-6:2013

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f9327-0aa9519684d8/sist-en-61131-6-2013>



IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable controllers –

Part 6: Functional safety

STANDARD PREVIEW

(standards.iteh.ai)

Automates programmables –

Partie 6: Sécurité fonctionnelle

SIST EN 61131-6:2013

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f-9327-0aa9519684d8/sist-en-61131-6-2013>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XD

ICS 25.040.40; 35.240.50

ISBN 978-2-83220-402-3

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.....	6
INTRODUCTION.....	8
1 Scope.....	10
2 Normative references	11
3 Terms and definitions	12
4 Conformance to this standard	25
5 FS-PLC safety lifecycle	25
5.1 General	25
5.2 FS-PLC functional safety SIL capability requirements.....	27
5.2.1 General	27
5.2.2 Data security	28
5.3 Quality management system.....	28
5.4 Management of FS-PLC safety lifecycle	29
5.4.1 Objectives	29
5.4.2 Requirements and procedures	29
5.4.3 Execution and monitoring	33
5.4.4 Management of functional safety	33
6 FS-PLC design requirements specification.....	33
6.1 General	33
6.2 Design requirements specification contents.....	34
6.3 Target failure rate.....	35
7 FS-PLC design, development and validation plan	36
7.1 General	36
7.2 Segmenting requirements.....	36
8 FS-PLC architecture	37
8.1 General	37
8.2 Architectures and subsystems	38
8.3 Data communication.....	38
9 HW design, development and validation planning	38
9.1 HW general requirements	38
9.2 HW functional safety requirements specification.....	38
9.3 HW safety validation planning	38
9.4 HW design and development	39
9.4.1 General	39
9.4.2 Requirements for FS-PLC behaviour on detection of a fault.....	39
9.4.3 HW safety integrity	40
9.4.4 Random HW failures.....	48
9.4.5 HW requirements for the avoidance of systematic failures	53
9.4.6 HW requirements for the control of systematic faults	53
9.4.7 HW classification of faults.....	54
9.4.8 HW implementation	55
9.4.9 De-rating of components.....	56
9.4.10 ASIC design and development.....	56
9.4.11 Techniques and measures to prevent the introduction of faults in ASICs	56

9.5	HW and embedded SW and FS-PLC integration	56
9.6	HW operation and maintenance procedures	57
9.6.1	Objective	57
9.6.2	Requirements	57
9.7	HW safety validation.....	58
9.7.1	General	58
9.7.2	Requirements	58
9.8	HW verification	59
9.8.1	Objective	59
9.8.2	Requirements	59
10	FS-PLC SW design and development	60
10.1	General	60
10.2	Requirements	61
10.3	Classification of engineering tools	61
10.4	SW safety validation planning.....	62
11	FS-PLC safety validation	62
12	FS-PLC type tests	62
12.1	General	62
12.2	Type test requirements	62
12.3	Climatic test requirements	65
12.4	Mechanical test requirements	65
12.5	EMC test requirements	65
12.5.1	General	65
12.5.2	General EMC environment.....	65
12.5.3	Specified EMC environment.....	67
13	FS-PLC verification	69
13.1	Verification plan	69
13.2	Fault insertion test requirements	70
13.3	As qualified versus as shipped	71
14	Functional safety assessment.....	71
14.1	Objective	71
14.2	Assessment requirements	72
14.2.1	Assessment evidence and documentation	72
14.2.2	Assessment method	72
14.3	FS-PLC assessment information.....	74
14.4	Independence.....	74
15	FS-PLC operation, maintenance and modification procedures	75
15.1	Objective	75
15.2	FS-PLC modification.....	75
16	Information to be provided by the FS-PLC manufacturer for the user	76
16.1	General	76
16.2	Information on conformance to this standard	76
16.3	Information on type and content of documentation.....	76
16.4	Information on catalogues and/or datasheets	76
16.5	Safety manual	76
16.5.1	General	76
16.5.2	Safety manual contents	76
Annex A	(informative) Reliability calculations.....	79

Annex B (informative) Typical FS-PLC Architectures.....	80
Annex C (informative) Energise to trip applications of FS-PLC.....	86
Annex D (informative) Available failure rate databases	88
Annex E (informative) Methodology for the estimation of common cause failure rates in a multiple channel FS-PLC.....	90
Bibliography.....	92
Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases.....	9
Figure 2 – Failure model.....	16
Figure 3 – FS-PLC safety lifecycle (in realization phase)	26
Figure 4 – Relevant parts of a safety function	35
Figure 5 – FS-PLC to engineering tools relationship	37
Figure 6 – HW subsystem decomposition.....	43
Figure 7 – Example: determination of the maximum SIL for specified architecture	45
Figure 8 – Example of limitation on hardware safety integrity for a multiple-channel safety function	47
Figure 9 – Fault classification and FS-PLC behaviour	54
Figure 10 – ASIC development lifecycle (V-Model).....	56
Figure 11 – Model of FS-PLC and engineering tools layers.....	60
Figure B.1 – Single FS-PLC with single I/O and external watchdog (1oo1D)	81
Figure B.2 – Dual PE with single I/O and external watchdogs (1oo1D).....	81
Figure B.3 – Dual PE with dual I/O, no inter-processor communication, and 1oo2 shutdown logic.....	82
Figure B.4 – Dual PE with dual I/O, inter-processor communication, and 1oo2D shutdown logic.....	83
Figure B.5 – Dual PE with dual I/O, no inter-processor communication, external watchdogs, and 2oo2 shutdown logic	83
Figure B.6 – Dual PE with dual I/O, inter-processor communication, external watchdogs, and 2oo2D shutdown logic	84
Figure B.7 – Triple PE with triple I/O, inter-processor communication, and 2oo3D shutdown logic.....	85
Table 1 – Safety integrity levels for low demand mode of operation	35
Table 2 – Safety integrity levels for high demand or continuous mode of operation	36
Table 3 – Faults to be detected and notified (alarmed) to the application program	40
Table 4 – Hardware safety integrity – low complexity (type A) subsystem	41
Table 5 – Hardware safety integrity – high complexity (type B) subsystem.....	41
Table 6 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction	50
Table 7 – Examples of tool classification.....	61
Table 8 – Performance criteria.....	64
Table 9 – Immunity test levels for enclosure port tests in general EMC environment.....	66
Table 10 – Immunity test levels in general EMC environment.....	67
Table 11 – Immunity test levels for enclosure port tests in specified EMC environment.....	68
Table 12 – Immunity test levels in specified EMC environment	69
Table 13 – Fault tolerance test, required effectiveness	71

Table 14 – Functional safety assessment Information	74
Table 15 – Minimum levels of independence of those carrying out functional safety assessment	75
Table E.1 – Criteria for estimation of common cause failure.....	90
Table E.2 – Estimation of common cause failure factor	91

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 61131-6:2013

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f-9327-0aa9519684d8/sist-en-61131-6-2013>

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61131-6 has been prepared by subcommittee 65B: Measurement and control devices, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this standard is based on the following documents:

FDIS	Report on voting
65B/831/FDIS	65B/850/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61131 series can be found, under the general title *Programmable controllers*, on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN 61131-6:2013

<https://standards.iteh.ai/catalog/standards/sist/abd150bb-52e3-492f-9327-0aa9519684d8/sist-en-61131-6-2013>