



SLOVENSKI STANDARD

SIST EN 61069-5:2017

01-marec-2017

Nadomešča:

SIST EN 61069-5:1998

Meritve, krmiljenje in avtomatizacija v industrijskih procesih - Ocenjevanje lastnosti sistema zaradi njegovega vrednotenja - 5. del: Vrednotenje zagotovljivosti sistema (IEC 61069-5:2016)

Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 5: Assessment of system dependability (IEC 61069-5:2016)

ITEH STANDARD PREVIEW
(standards.iteh.ai)

Leittechnik für industrielle Prozesse - Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems - Teil 5: Eignungsbeurteilung der Systemzuverlässigkeit (IEC 61069-5:2016)

<https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017>

Mesure, commande et automation dans les processus industriels - Appréciation des propriétés d'un système en vue de son évaluation - Partie 5: Evaluation de la sûreté de fonctionnement d'un système (IEC 61069-5:2016)

Ta slovenski standard je istoveten z: EN 61069-5:2016

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
-----------	--	--

SIST EN 61069-5:2017

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 61069-5:2017](https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017)

<https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017>

EUROPEAN STANDARD

EN 61069-5

NORME EUROPÉENNE

EUROPÄISCHE NORM

September 2016

ICS 25.040.40

Supersedes EN 61069-5:1995

English Version

**Industrial-process measurement, control and automation -
Evaluation of system properties for the purpose of system
assessment - Part 5: Assessment of system dependability
(IEC 61069-5:2016)**

Mesure, commande et automation dans les processus industriels - Appréciation des propriétés d'un système en vue de son évaluation - Partie 5: Evaluation de la sûreté de fonctionnement d'un système
(IEC 61069-5:2016)

Leittechnik für industrielle Prozesse - Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems - Teil 5: Eignungsbeurteilung der Systemzuverlässigkeit
(IEC 61069-5:2016)

This European Standard was approved by CENELEC on 2016-07-20. 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.



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/793/FDIS, future edition 2 of IEC 61069-5, 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 61069-5:2016.

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) 2017-04-20
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2019-07-20

This document supersedes EN 61069-5:1995.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Endorsement notice

[SIST EN 61069-5:2017](https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017)

[https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-](https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017)

[1838d70c2b08/sist-en-61069-5-2017](https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017)

The text of the International Standard IEC 61069-5:2016 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 60300-3-1:2003	NOTE	Harmonized as EN 60300-3-1:2004 (not modified).
IEC 60068	NOTE	Harmonized in EN 60068 series.
IEC 60812:2006	NOTE	Harmonized as EN 60812:2006 (not modified).
IEC 61000	NOTE	Harmonized in EN 61000 series.
IEC 61025:2006	NOTE	Harmonized as EN 61025:2007 (not modified).
IEC 61069-6	NOTE	Harmonized as EN 61069-6.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 61165	NOTE	Harmonized as EN 61165.
IEC 61326	NOTE	Harmonized in EN 61326 series.
IEC 61508	NOTE	Harmonized in EN 61508 series.

IEC 62443	NOTE	Harmonized in EN 62443 series ¹⁾ .
IEC/TS 62603-1	NOTE	Harmonized as CLC/TS 62603-1.

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN 61069-5:2017

<https://standards.iteh.ai/catalog/standards/sist/642b9af8-4118-41ed-ae9e-1838d70c2b08/sist-en-61069-5-2017>

1) At draft stage.

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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60300-3-2	-	Dependability management - Part 3-2: Application guide - Collection of dependability data from the field	EN 60300-3-2	-
IEC 60319	-	Presentation and specification of reliability data for electronic components	-	-
IEC 61069-1	2016	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 1: Terminology and basic concepts	EN 61069-1	201X ²⁾
IEC 61069-2	2016	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 2: Assessment methodology	EN 61069-2	201X ²⁾
IEC 61070	-	Compliance test procedures for steady- state availability	-	-
IEC 61709	2011	Electric components - Reliability - Reference conditions for failure rates and stress models for conversion	EN 61709	2011
ISO/IEC 25010	-	Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models	-	-
ISO/IEC 27001	2013	Information technology - Security techniques - Information security management systems - Requirements	-	-
ISO/IEC 27002	-	Information technology - Security techniques - Code of practice for information security controls	-	-

2) To be published.



IEC 61069-5

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability

Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 5: Évaluation de la sûreté de fonctionnement d'un système

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-3447-1

**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.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references.....	8
3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols.....	9
3.1 Terms and definitions.....	9
3.2 Abbreviated terms, acronyms, conventions and symbols.....	9
4 Basis of assessment specific to dependability.....	9
4.1 Dependability properties.....	9
4.1.1 General.....	9
4.1.2 Availability.....	10
4.1.3 Reliability.....	10
4.1.4 Maintainability.....	10
4.1.5 Credibility.....	11
4.1.6 Security.....	11
4.1.7 Integrity.....	12
4.2 Factors influencing dependability.....	12
5 Assessment method.....	12
5.1 General.....	12
5.2 Defining the objective of the assessment.....	12
5.3 Design and layout of the assessment.....	13
5.4 Planning of the assessment program.....	13
5.5 Execution of the assessment.....	13
5.6 Reporting of the assessment.....	13
6 Evaluation techniques.....	13
6.1 General.....	13
6.2 Analytical evaluation techniques.....	14
6.2.1 Overview.....	14
6.2.2 Inductive analysis.....	15
6.2.3 Deductive analysis.....	15
6.2.4 Predictive evaluation.....	15
6.3 Empirical evaluation techniques.....	16
6.3.1 Overview.....	16
6.3.2 Tests by fault-injection techniques.....	16
6.3.3 Tests by environmental perturbations.....	17
6.4 Additional topics for evaluation techniques.....	17
Annex A (informative) Checklist and/or example of SRD for system dependability.....	18
Annex B (informative) Checklist and/or example of SSD for system dependability.....	19
B.1 SSD information.....	19
B.2 Check points for system dependability.....	19
Annex C (informative) An example of a list of assessment items (information from IEC TS 62603-1).....	20
C.1 Overview.....	20
C.2 Dependability.....	20
C.3 Availability.....	20

C.3.1	System self-diagnostics.....	20
C.3.2	Single component fault tolerance and redundancy	20
C.3.3	Redundancy methods.....	21
C.4	Reliability.....	22
C.5	Maintainability.....	23
C.5.1	General	23
C.5.2	Generation of maintenance requests	23
C.5.3	Strategies for maintenance.....	23
C.5.4	System software maintenance	23
C.6	Credibility	23
C.7	Security	24
C.8	Integrity	24
C.8.1	General	24
C.8.2	Hot-swap	24
C.8.3	Module diagnostic	24
C.8.4	Input validation	24
C.8.5	Read-back function	24
C.8.6	Forced output	24
C.8.7	Monitoring functions.....	24
C.8.8	Controllers.....	24
C.8.9	Networks	25
C.8.10	Workstations and servers.....	25
Annex D (informative)	Credibility tests.....	26
D.1	Overview.....	26
D.2	Injected faults.....	27
D.2.1	General	27
D.2.2	System failures due to a faulty module, element or component.....	27
D.2.3	System failures due to human errors	27
D.2.4	System failures resulting from incorrect or unauthorized inputs into the system through the man-machine interface	27
D.3	Observations.....	28
D.4	Interpretation of the results.....	28
Annex E (informative)	Available failure rate databases	29
E.1	Databases	29
E.2	Helpful standards concerning component failure	30
Annex F (informative)	Security considerations	31
F.1	Physical security	31
F.2	Cyber-security.....	31
F.2.1	General	31
F.2.2	Security policy	31
F.2.3	Other considerations.....	31
Bibliography	33
Figure 1 – General layout of IEC 61069	7
Figure 2 – Dependability	9

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION –
EVALUATION OF SYSTEM PROPERTIES FOR
THE PURPOSE OF SYSTEM ASSESSMENT –****Part 5: Assessment of system dependability**

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 61069-5 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1994. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) reorganization of the material of IEC 61069-5:1994 to make the overall set of standards more organized and consistent;
- b) IEC TS 62603-1 has been incorporated into this edition.

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

FDIS	Report on voting
65A/793/FDIS	65A/803/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 in the IEC 61069 series, published under the general title *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment*, can be found 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)

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

IEC 61069 deals with the method which should be used to assess system properties of a basic control system (BCS). IEC 61069 consists of the following parts.

- Part 1: Terminology and basic concepts
- Part 2: Assessment methodology
- Part 3: Assessment of system functionality
- Part 4: Assessment of system performance
- Part 5: Assessment of system dependability
- Part 6: Assessment of system operability
- Part 7: Assessment of system safety
- Part 8: Assessment of other system properties

Assessment of a system is the judgement, based on evidence, of the suitability of the system for a specific mission or class of missions.

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the specific mission or class of missions.

Since this is rarely practical, the rationale on which an assessment of a system should be based is:

- the identification of the importance of each of the relevant system properties,
- the planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various system properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of a system within practical cost and time constraints.

An assessment can only be carried out if a mission has been stated (or given), or if any mission can be hypothesized. In the absence of a mission, no assessment can be made; however, evaluations can still be specified and carried out for use in assessments performed by others. In such cases, IEC 61069 can be used as a guide for planning an evaluation and it provides methods for performing evaluations, since evaluations are an integral part of assessment.

In preparing the assessment, it can be discovered that the definition of the system is too narrow. For example, a facility with two or more revisions of the control systems sharing resources, for example a network, should consider issues of co-existence and inter-operability. In this case, the system to be investigated should not be limited to the “new” BCS; it should include both. That is, it should change the boundaries of the system to include enough of the other system to address these concerns.

The series structure and the relationship among the parts of IEC 61069 are shown in Figure 1.

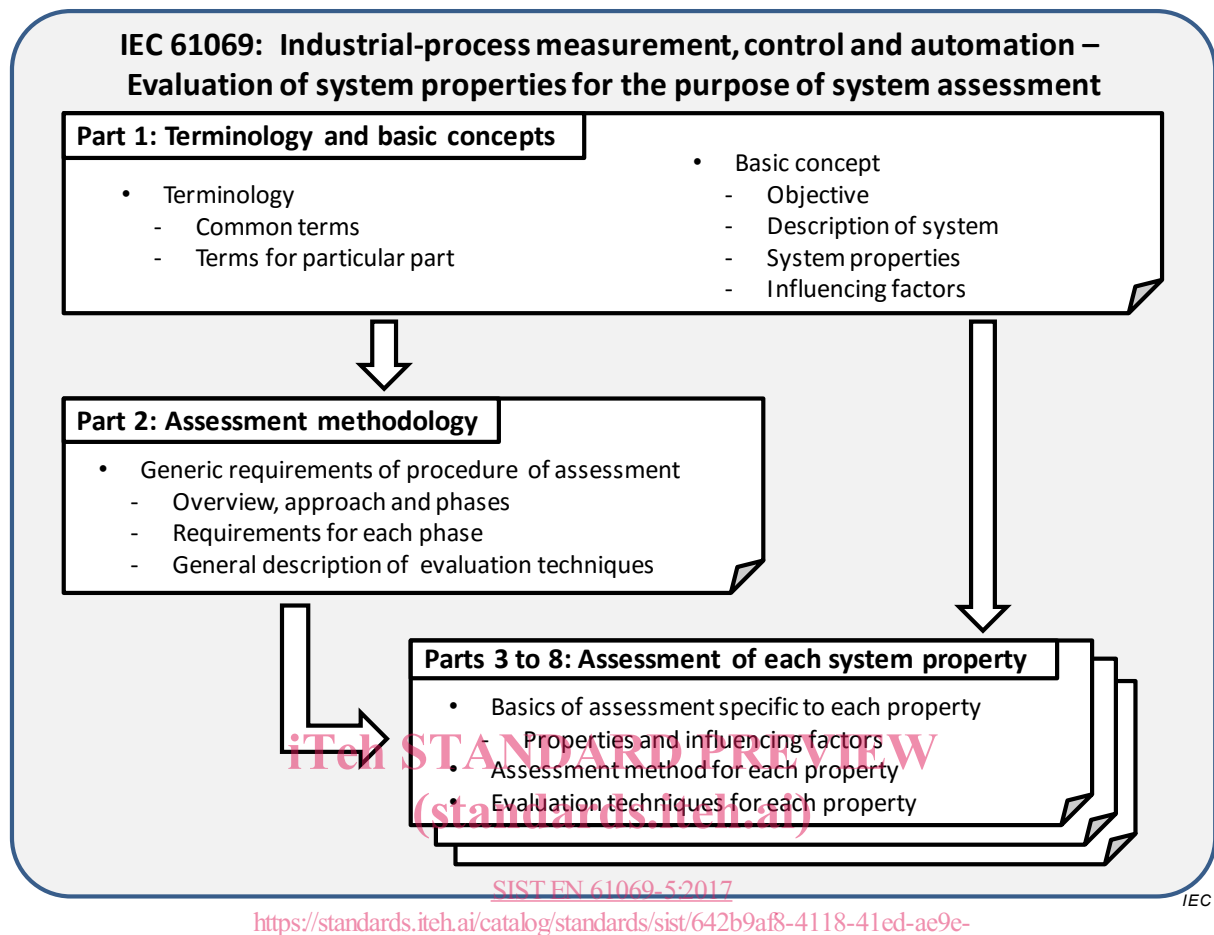


Figure 1 – General layout of IEC 61069

Some example assessment items are integrated in Annex C.