IEC 61069-5

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

IEC 61069-5:2016-06(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 61069-5

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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.

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.

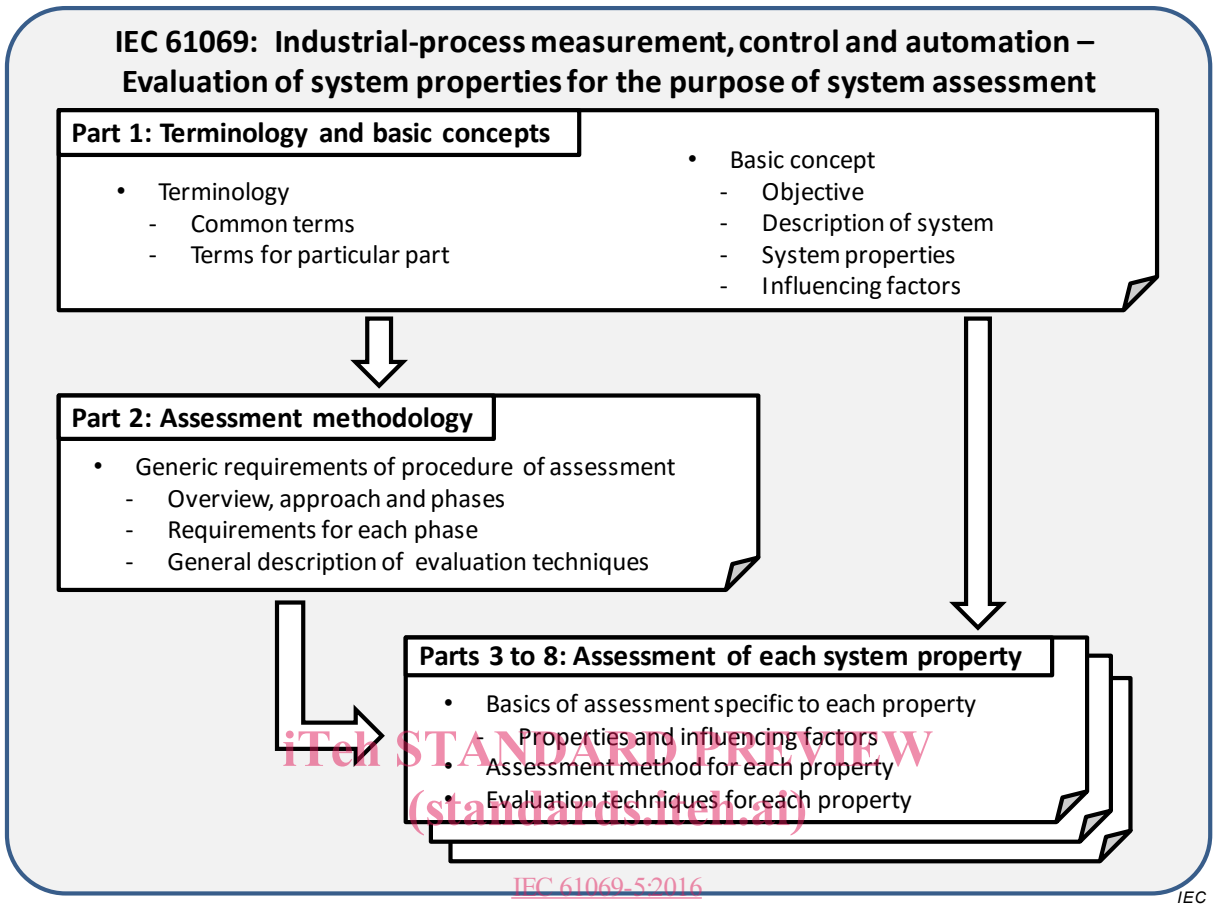

Figure 1 – General layout of IEC 61069

Some example assessment items are integrated in Annex C.

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 5: Assessment of system dependability

1 Scope

This part of IEC 61069:

– specifies the detailed method of the assessment of dependability of a basic control system (BCS) based on the basic concepts of IEC 61069-1 and methodology of IEC 61069-2,

– defines basic categorization of dependability properties,

– describes the factors that influence dependability and which need to be taken into account when evaluating dependability, and

– provides guidance in selecting techniques from a set of options (with references) for evaluating the dependability.

2 Normative references

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.

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

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*

IEC 61069-2:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

IEC 61070, *Compliance test procedures tor steady-state availability*

IEC 61709:2011, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

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*

3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61069-1 apply.

3.2 Abbreviated terms, acronyms, conventions and symbols

For the purposes of this document, the abbreviated terms, acronyms, conventions and symbols given in IEC 61069-1 apply.

4 Basis of assessment specific to dependability

4.1 Dependability properties

4.1.1 General

To fully assess the dependability, the system properties are categorised in a hierarchical way.

For a system to be dependable it is necessary that it is ready to perform its functions. However, in practice, when the system is ready to perform its function, this does not mean that it is sure that the functions are performed correctly. In order to cover these two aspects, dependability properties are categorised into the groups and subgroups shown in Figure 2.

Figure 2 – Dependability

Dependability cannot be assessed directly and cannot be described by a single property. Dependability can only be determined by analysis and testing of each of its properties individually.

The relationship between the dependability properties of the system and its modules is sometimes very complex.

For example:

– if the system configuration includes redundancy, availability property of the system is dependent upon the integrity properties of the redundant modules;
– if the system configuration includes system security mechanisms, security property of the system is dependent upon the availability properties of modules that perform the security mechanism;
– if the system configuration includes modules that check data transferred internally from other parts of the system, then integrity property of the system is dependent upon the security properties of these modules.

When a system performs several tasks of the system, its dependability can vary across those tasks. For each of these tasks, a separate analysis is required.

4.1.2 Availability

Availability of the system is dependent upon the availabilities of the individual modules of the system and the way in which these modules cooperate in performing tasks of the system. The way in which modules of the system cooperate can include functional redundancy (homogeneous or diverse), functional fall-back and degradation. Availability is dependent in practice upon the procedures used and the resources available for maintaining the system. The availability of the system can differ with respect to each of its tasks.

Availability of the system for each task can be quantified in two ways:

A system's availability can be predicted as:

Availability = mean_time_to_failure / (mean_time_to_failure + mean_time_to_restoration)

where:

- "availability" is the availability of the system for the given task;
- "mean_time_to_failure" is the mean of the time from restoration of a system into a state of performing its given task(s) to the time the system fails to do so;
- "mean-time_to_restoration" is the mean of the total time required to restore performance of the given task from the time the system failed to perform that task.

For a system in operation, the availability can be calculated as:

Availability = total_time_the_system_has_been_able_to_perform_the_task / Total_time_the_system_has_been_expected_to_perform_the_task

4.1.3 Reliability

Reliability of a system is dependent upon the reliability of the individual modules of the system and the way in which these modules cooperate in performing task(s) of the system. The way in which these modules cooperate can include functional redundancy (homogeneous or diverse), functional fall-back and degradation.

Reliability of the system can differ with respect to each of its tasks. Reliability can be quantified for individual tasks, with varying degrees of predictive confidence.

The reliability of the individual elements of the system can be predicted using the parts count method (see IEC 62380 and IEC 61069-6). Reliability of the system can then be predicted by synthesis. It should be noted, that for the software modules of systems, there are no reliability prediction methods available that provide high levels of confidence.

Mechanisms to analyse software reliability are described in ISO IEC 25010.

Reliability can be represented by mean time to failure (MTTF) or failure rate.

4.1.4 Maintainability

The maintainability of a system is dependent upon the maintainability of individual elements and structure of elements and modules of the system. The physical structure affects ease of access, replaceability, etc. The functional structure affects ease of diagnosis, etc.

When quantifying the maintainability of a system, all actions required to restore the system to the state where it is fully capable of performing its tasks should be included. This should include actions such as the time necessary to detect the fault, to notify maintenance, to diagnose and remedy the cause, to adjust and check, etc.

The quantification of maintainability should be augmented with qualitative statements by checking the provision for and the coverage of the following items:

The quantification of maintainability should be augmented with qualitative statements by checking the provision for and the coverage of the following items:

– notification of the occurrence of the failures: lights, alert messages, reports, etc.;
– access: ease of access for personnel and for connecting measuring instruments, modularity, etc.;
– diagnostics: direct fault identification, diagnostic tools which have no influence on the system by itself, remote maintenance support facilities, statistical error checking and reporting;
– repairability/replaceability: few restrictions on the replacement of modules while operating ("hot swap" support), modularity, unambiguous identification of modules and elements, minimum need for special tools, minimum repercussions on other elements or modules, when elements or modules are replaced;
– check-out: guided maintenance procedures, minimum check-out requirements.

Maintainability can be represented by mean time to repair (MTTR).

4.1.5 Credibility

The credibility of a system is dependent upon the integrity and security mechanisms implemented as functions performed by the modules of the system.

Credibility mechanisms include:

– a check on
  - correct performance of functions (for example by watchdog, using known data); and/or
  - correct data (for example validity check, parity check, readback, input validation, etc.);
– an action, such as:
  - self-correction;
  - confinement;
  - notification of action, etc.

These mechanisms can be used to provide integrity and/or security.

To analyse the credibility mechanisms, the fault injection techniques described in 6.1 can be used.

Credibility is deterministic and some aspects can be quantified.

4.1.6 Security

The security of a system is dependent upon mechanisms implemented at the boundary of the system to detect and prevent incorrect inputs and unauthorized access. These boundaries can be physical or virtual. See:

– Annex F for more considerations on security, and
– IEC 62443 series.

A security mechanism can be implemented by an element checking the inputs to other elements.

4.1.7 Integrity

The integrity is dependent upon mechanisms implemented at the output elements of the system to check for correct outputs. It also depends upon mechanisms implemented within the system to detect and prevent incorrect transitions of signals or data between parts of the system.

An integrity mechanism is implemented by an element checking the outputs of other elements.

4.2 Factors influencing dependability

The dependability of a system can be affected by the following influencing factors listed in IEC 61069-1:2016, 5.3.

For each of the system properties listed in 4.1, the primary influencing factors are as follows:

– Reliability is influenced by the influencing factors;
  - utilities, the influence is partly predictable using IEC 61709,
  - environment, the influence is partly predictable using IEC 61709,
  - services, due to the handling, storage of parts, etc.
– Maintainability; for the purpose of this standard, maintainability is considered as an intrinsic property of the system itself and is only affected in an indirect way, for example restricted access due to hazardous conditions.
– Availability; when taking into account the human activities necessary to retain the system in, or restore the system to, a state in which the system is capable of performing task(s) of the system, availability is influenced by human behaviour and service conditions (delays in delivery of spare parts, training, documentation, etc.).
– Credibility; the mechanisms (security and integrity) can be affected by intentional or unintentional human actions and by infestations of pests and if these mechanisms share common facilities, such as buses or multitasking processors, they can be influenced by task(s) of the system, the process due to a sudden increase in process activity (for example an alarm burst), etc. and external systems.

In general, any deviations from the reference conditions in which the system is supposed to operate can affect the correct working of the system.

When specifying tests to evaluate the effects of influencing factors, the following standards should be consulted:

– IEC 60068,
– IEC 60801,
– IEC 61000, and
– IEC 61326.

5 Assessment method

5.1 General

The assessment shall follow the method as laid down in IEC 61069-2:2016, Clause 5.

5.2 Defining the objective of the assessment

Defining the objective of the assessment shall follow the method as laid down in IEC 61069-2:2016, 5.2.

5.3 Design and layout of the assessment

Design and layout of the assessment shall follow the method as laid down in IEC 61069-2:2016, 5.3.

Defining the scope of assessment shall follow the method laid down in IEC 61069-2:2016, 5.3.1.

Collation of documented information shall be conducted in accordance with IEC 61069-2:2016, 5.3.3.

The statements compiled in accordance with IEC 61069-2:2016, 5.3.3 should include the following in addition to the items listed in IEC 61069-2:2016, 5.3.3.

– No additional items are noted

Documenting collated information shall follow the method in IEC 61069-2:2016, 5.3.4.

Selecting assessment items shall follow IEC 61069-2:2016, 5.3.5.

Assessment specification should be developed in accordance with IEC 61069-2:2016, 5.3.6.

Comparison of the SRD and the SSD shall follow IEC 61069-2:2016, 5.3.

NOTE 1 A checklist of SRD for system dependability is provided in Annex A.

NOTE 2 A checklist of SSD for system dependability is provided in Annex B.

5.4 Planning of the assessment program

Planning the assessment program shall follow the method as laid down in IEC 61069-2:2016, 5.4.

Assessment activities shall be developed in accordance with IEC 61069-2:2016, 5.4.2.

The final assessment program should specify points specified in IEC 61069-2:2016, 5.4.3.

5.5 Execution of the assessment

The execution of the assessment shall be in accordance with IEC 61069-2:2016, 5.5.

5.6 Reporting of the assessment

The reporting of the assessment shall be in accordance with IEC 61069-2:2016, 5.6.

The report shall include information specified in IEC 61069-2:2016, 5.6. Additionally, the assessment report should address the following points:

– No additional items are noted.

6 Evaluation techniques

6.1 General

Within this standard, several evaluation techniques are suggested. Other methods may be applied but, in all cases, the assessment report should provide references to documents describing the techniques used.

Those evaluation techniques are categorized as described in IEC 61069-2:2016, Clause 6.