Irish Standard
I.S. EN 50271:2018

Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen - Requirements and tests for apparatus using software and/or digital technologies

I.S. EN 50271:2018

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
EN 50271:2018	2018-06-15

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2018-07-24	13.320
	NOTE: If blank see CEN/CENELEC cover page

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

National Foreword

I.S. EN 50271:2018 is the adopted Irish version of the European Document EN 50271:2018, Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen - Requirements and tests for apparatus using software and/or digital technologies

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50271

June 2018

ICS 13.320

Supersedes EN 50271:2010

English Version

Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen - Requirements and tests for apparatus using software and/or digital technologies

Appareils électriques de détection et de mesure des gaz combustibles, des gaz toxiques ou de l'oxygène - Exigences et essais pour les appareils utilisant un logiciel et/ou des technologies numériques

Elektrische Geräte für die Detektion und Messung von brennbaren Gasen, giftigen Gasen oder Sauerstoff - Anforderungen und Prüfungen für Warngeräte, die Software und/oder Digitaltechnik nutzen

This European Standard was approved by CENELEC on 2017-11-06. 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, 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

Ref. No. EN 50271:2018 E

Contents

European foreword

This document (EN 50271:2018) has been prepared by CLC/SC 31-9, “Electrical apparatus for the detection and measurement of combustible gases to be used in industrial and commercial potentially explosive atmospheres”, of CLC/TC 31, “Electrical apparatus for potentially explosive atmospheres”, and by CLC/TC 216 “Gas detectors”.

The following dates are fixed:

- latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2018-12-15
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2021-06-15

This document supersedes EN 50271:2010.

The State of the Art is included in Annex ZY “*Significant changes between this European Standard and* EN 50271:2010” which lists all changes to EN 50271:2010.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EU Directive 2014/34/EU.

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

Introduction

This European Standard specifies minimum requirements for functional safety of gas detection apparatus using software and/or digital technologies and defines criteria for reliability and avoidance of faults. Functional safety is that part of the overall safety which is related to the measures within the gas detection apparatus to avoid or to handle failures in such a manner that the safety function will be ensured.

Gas detection apparatus will fail to function if dangerous failures occur. The aim of this European Standard is to reduce the risk of dangerous equipment failures to levels appropriate to typical applications of such apparatus.

Failure to function will also occur if such apparatus are not selected, installed or maintained in an appropriate manner. In some applications failures of this type will dominate the functional safety achieved. Users of gas detection apparatus will therefore need to ensure that selection, installation and maintenance of such apparatus are carried out appropriately. Guidance for the selection, installation, use and maintenance of gas detection apparatus are set out in EN 60079-29-2 and EN 45544-4, respectively.

This European Standard does not include requirements for operational availability which will need to be considered separately.

Regarding the requirements for the software development process, this European Standard specifies a practical approach to comply with the requirements of EN 61508-3 for SIL 1 without using this generic standard.

This European standard also specifies additional optional requirements for compliance with SIL 1 in low demand mode operation. The following apparatus or gas detection systems are not fully covered by this standard:

– apparatus at SIL 1 when the apparatus or gas detection system contains functionality not covered by EN 50271

– apparatus at SIL 1 high demand mode operation

– apparatus at SIL 2 and SIL 3;

For such apparatus or gas detection systems the European standard EN 50402 should be used instead of EN 50271. EN 50402 includes all requirements of EN 50271.

1 Scope

This European Standard specifies minimum requirements and tests for electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen using software and/or digital technologies.

This European Standard is applicable to fixed, transportable and portable apparatus intended for use in domestic premises as well as commercial and industrial applications and their software-controlled safety related accessories.

This European Standard does not apply to external sampling systems which are not accessories, or to apparatus of laboratory or scientific type, or to apparatus used only for process control purposes.

This European Standard supplements the requirements of the European Standards for the detection and measurement of flammable gases and vapours (e.g. EN 60079-29-1, EN 60079-29-4, EN 50194-1, EN 50194-2), toxic gases (e.g. EN 45544 series, EN 50291-1, EN 50291-2) or oxygen (e.g. EN 50104).

NOTE 1 These European Standards will be mentioned in this European Standard as “metrological standards”.

NOTE 2 The examples above show the state of the standardization for gas detection apparatus at the time of publishing this European Standard. There may be other metrological standards for which this European Standard is also applicable.

This European Standard is a product standard which is based on the EN 61508 series. It covers part of the phase 10 “realisation” of the overall safety life cycle defined in EN 61508-1.

Additional requirements are specified if compliance with safety integrity level 1 (SIL 1) according to the EN 61508 series is claimed for fixed or transportable apparatus for low demand mode of operation. They can also be applied to portable apparatus which are able to perform an automatic executive action.

It is recommended to apply this European Standard for apparatus used for safety applications with SIL-requirement 1 instead of EN 50402. However, the technical requirements of EN 50271 and EN 50402 are the same for SIL 1.

NOTE 3 For apparatus used for safety applications with SIL-requirements higher than 1 EN 50402 is applicable.

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.

EN 50402:2017, *Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen - Requirements on the functional safety of gas detection systems*

EN 60079-29-1:2016, *Explosive atmospheres - Part 29-1: Gas detectors - Performance requirements of detectors for flammable gases*

EN 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements*

EN 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 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements*

EN 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations*

EN 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels*

EN 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 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 60079-29-1:2016 and the following apply.

3.1
digital unit
part of an electrical apparatus in which data is processed digitally. Analogue-digital(A/D)-converters and digital-analogue(D/A)-converters as interfaces to analogue units of the apparatus belong to the digital unit

3.2
special state
all states of the apparatus other than those in which monitoring of gas concentration and/or alarming is intended, for example the special states of warm-up, calibration mode or fault condition

[SOURCE: EN 60079-29-1:2016, 3.5.4]

3.3
software
intellectual creation comprising the programs, procedures, rules and associated documentation pertaining to the operation of the digital unit

3.4
failure
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

[SOURCE: EN 61508-4:2010, 3.6.4, mod.]

3.5
parameters
settings by the manufacturer or user which affect the operation of the apparatus, e.g. changing of the alarm set points or measuring ranges. Parameter options are included in the hardware and/or software during design of the apparatus. Changes of parameter settings are not modifications of the software. In the software several different levels of permission to read or to change parameters may exist

3.6
specified range of input values
range of analogue input values corresponding to the digital output range of an A/D-converter or range of digital input values corresponding to the analogue output range of a D/A-converter. The minimum and maximum digital values of the converter are not to be considered to be within the specified range because minima and maxima correspond to stuck-at faults which have to be detected by the apparatus (see 4.1.4)

3.7
defined range of input values
range of input values defined by the manufacturer of the apparatus to be valid; the defined range is a sub-range of the specified range of input values

3.8
output data
result of the digital data processing, which is used for driving the output interfaces

Note 1 to entry: Output interfaces may be analogue or digital displays, analogue or digital outputs and/or alarm indicators or relays.

3.9
output signal
analogue or digital signal which is available at an output interface

3.10
measured value
processed measured signal including physical unit (e.g. % LEL). A measured value may be formed from a single signal or a combination of several measured signals. The combined measured signals may represent different physical units, e.g. gas concentration and temperature

3.11
smallest deviation of indication
value which is determined by the applicable metrological standards. In metrological standards the allowed tolerances for deviation of indication during type testing are given. If there are different requirements for the tolerances in different applicable metrological standards the smallest tolerance is the “smallest deviation of indication”

Note 1 to entry: The smallest deviation of indication is basis for the required resolution of measured signals which use digital transmission and data processing to meet the requirements of the metrological standards when using digital technologies

[SOURCE: EN 50402:2017, 3.22]

3.12
message
indication on a display which gives an information about the status of the apparatus (e.g. alarm, special state, warning)

3.13
software component
part of the program that consists of one or several software modules and that can also interact with other such constructs

3.14
software module
construct that consists of subroutines and/or data declarations and that can also interact with other such constructs

3.15
safety function of a gas detection apparatus
any function (inclusive from gas sampling to output of the gas detection apparatus) implemented by the gas detection apparatus which is related to safety as defined by the manufacturer

4 Design principles

4.1 Basic requirements

4.1.1 General

The metrological standards define performance requirements for gas detection apparatus which have direct implications on the digital units and software which may be used in such apparatus. This subclause specifies basic requirements to digital units and software to fulfil the metrological standards.

4.1.2 Analogue/digital interface

The relationship between corresponding analogue and digital values shall be unambiguous. The output range shall be capable of coping with the defined range of input values. Input values outside the specified range of the converter shall not result in a valid measured value. A/D- and D/A-converter quantisation steps shall be chosen so that the requirements in 4.1.3 for the accuracy of data representation will be fulfilled. The design shall take into account the maximum possible A/D- and D/A-converter errors.

NOTE This assessment need not include environmental interferences to the A/D- or D/A-converters, e.g. temperature variation, since environmental testing is covered by the metrological standards.

Outputs at the limits of the specified range of D/A-converters shall result in output signals which are described as fault signal by the manufacturer.

4.1.3 Numerical errors

Deviations of measured values arising from quantisation, rounding and calculation errors shall be estimated assuming worst case conditions.

These worst case conditions shall be evaluated in detail. For example, nonlinear behaviour of the sensor signal with gas concentration, ageing of sensors, varying sensitivities for different gases and signal variation with temperature, pressure or humidity shall be taken into consideration.

The estimated deviation of measured values shall not be greater than 50 % of the smallest deviation of indication.

NOTE The deviation of measured values arising from the digital unit will be typically much lower than 50 % of the smallest deviation of indication. Deviations arising from other sources (e.g. sensor) are expected to be dominant.

4.1.4 Measuring operation

During data processing the digital unit shall automatically control the specified input data range and handle range violations. The minimum and maximum digital values of the converter shall not be considered to be within the specified range in order to detect stuck-at faults.

The software design and verification shall guarantee that range violations for internal and output data do not occur. Otherwise the digital unit shall automatically control the allowed data ranges and handle range violations.

During measuring operation, the maximum overall time of four successive updates of the measured value and all safety relevant output signals shall not exceed the response time t_{90} of the apparatus or, for alarm only apparatus, the minimum time to alarm.

NOTE This timing requirement may not be applied to output signals which are explicitly claimed by the manufacturer to be not safety-relevant.

4.1.5 Special state indication

4.1.5.1 General

It shall not be possible for any interface to an external device to adversely affect a safety function of the apparatus without the apparatus entering a special state.

NOTE This includes both hardware and software interfaces.

4.1.5.2 Fixed and transportable apparatus

a) Control units

While a special state is present within the entire gas detection apparatus (i.e. control unit and external sensors or transmitters) this shall be continuously indicated by a signal. This signal shall be transmittable except when the apparatus is intended to be used in domestic premises only. Signals provided for indicating that the entire gas detection apparatus is in the special state “fault” shall be such that they de-energize when the special state occurs and also on power loss. In the case of deactivation of alarm devices, e.g. for calibration purposes, it is not required to indicate a special state by a transmittable signal if the alarm devices are automatically re-enabled within 15 min.

b) Gas detection transmitters intended to be used with control units

The special state “calibration” shall be transmitted to the control unit continuously or the measured value shall be transmitted during calibration. All other special states shall be transmitted to the control unit continuously. The test routine according to 4.6 c) is excluded.

c) All other apparatus

A special state shall be continuously indicated by a signal. This signal shall be transmittable except when the apparatus is intended to be used in domestic premises only. Signals provided for indicating that the apparatus is in the special state “fault” shall be such that they de-energize when the special state occurs and also on power loss. In the case of deactivation of alarm devices, e.g. for calibration purposes, it is not required to indicate a special state by a transmittable signal if the alarm devices are automatically re-enabled within 15 min.

In the case of digital data transmission, the term “continuously” is used with the meaning: continually, at the rate at which the output signal is updated (see 4.1.4).

4.1.5.3 Portable apparatus

The special state “fault” shall be continuously indicated by an optical and audible signal. It is permitted that the audible signal can be silenced.

If it is not possible to show an indication in all possible fault situations the normal operation of the apparatus shall be confirmed by a periodic optical and audible output signal (commonly called alive signal or confidence signal). The time interval between two signals shall not exceed 60 s.

EXAMPLE: A sudden breakdown of battery voltage cannot be indicated without implementing a second independent power supply.

The special state “warm-up” shall be indicated by an optical and/or audible signal.

The special states “calibration mode” and “parameterization mode” shall be indicated by an optical signal.

4.2 Displays

4.2.1 General

If a display is provided the requirements of 4.2.2 and 4.2.3 apply.

4.2.2 Indication of messages

If it is intended to indicate messages on a display:

a) it shall be possible to display all active messages simultaneously or a consolidated signal shall be generated (e.g. indicating lights for alarms or fault) and a consolidated message shall be displayed. It shall be possible to interrogate all active messages;

b) a unique message shall be provided for each individual gas alarm;

c) if no special state is activated, it shall be possible to interrogate the measured values of all gas sensors.

If a message includes another subsidiary message (e.g. exceeding the 2nd alarm threshold includes exceeding the 1st alarm threshold) it is sufficient to show the message of higher priority. After cancelling the higher order message the subsidiary message shall remain if the reason for its activation still exists.

It is recommended that the manufacturer defines an appropriate set of messages in order to enable the user an easy identification of alarms, special states, etc.

4.2.3 Indication of measured values

For measured values the displayed unit of measurement and any related sign shall be unambiguous. Any under-range or over-range measurements shall be clearly indicated according to the requirements of the metrological standards.

4.3 Software

4.3.1 General

This clause specifies minimum requirements for the software development process which are based on EN 61508-3. Alternative procedures are permitted provided that the applicable requirements of EN 61508-3 are fulfilled. Compliance through “proven in use” (Route 2s of EN 61508-3) shall not be used.

NOTE This standard specifies minimum requirements and does not give additional recommendations (in the tables of EN 61508-3 and in EN 50402:2017 marked as “R”).

In general, software will consist of device software and, if applicable, an operating system and libraries (e.g. mathematical functions).

The requirements of this clause shall be applied to the entire software. A distinction between safety-related and non safety-related software is not made.

New operating systems shall be developed according to 4.3.3 to 4.3.5. Re-used or commercial operating systems shall comply with 4.3.2.

New device software and libraries shall be developed according to 4.3.3 to 4.3.5.

Bought or re-used software modules which were previously developed according to 4.3.3 to 4.3.5 or commercial libraries which are only available as object code shall be qualified (see 4.3.5.3.2).

Bought or re-used software modules which are relevant for the basic gas detection functionality (signal chain from sensor to safety relevant output(s)) or the effectiveness of the test routines (according to 4.6) which were not developed according to 4.3.3 to 4.3.5 shall be treated as new code (Route 3s according to EN 61508-3, 7.4.2.13). All other bought or re-used software modules shall be qualified (see 4.3.5.3.2).

Only the requirements of 4.3.3, 4.3.4 a)-e), g), h) and 4.7 shall be applied to software for parameterization of the gas detection device, which is running on external devices (e.g. PC) on request and under control of an authorized user for a short period of time.

4.3.2 Re-used or commercial operating systems

4.3.2.1 Requirements

Re-used or commercial operating systems may be integrated without applying 4.3.3 to 4.3.5 if the following requirements are fulfilled:

a) quasi-real time capability for compliance with the requirements of 4.1.4;

b) it shall not be possible for the user to modify the configuration of the operating system;

c) no automatic update-function for the operating system;

d) upgrades of the operating system shall only be possible under the control of the manufacturer of the apparatus;

e) if the program is executed from volatile memory the entire software shall be fully loaded at start-up of the apparatus. In special states which are entered by a deliberate action of the user (e.g. modification of parameters) loading of further modules is permitted;

f) functional safety is validated to be at least SIL 1 according to EN 61508-3 or the operating system is used with the restrictions according to 4.3.2.2.

It is pointed out that, according to 4.3.5.9, in case of modification of the operating system the impact on the device software shall be assessed and, if necessary, modification and validation procedures shall be performed.

4.3.2.2 Use of operating systems without validation of functional safety

An operating system without validation of functional safety is permitted to be used if the following requirements are fulfilled.

a) The device software has a logical and temporal monitoring of program sequence.

b) The monitoring equipment according to 4.6 d) is triggered by the device software only (that is, the device software operates the hardware IO ports and watchdog directly, without using the operating system).

c) Output ports which are part of the safety function are exclusively driven by the device software. However, functions of the operating system may be used if the correct settings of the output ports are verified by the device software.

d) Input ports which are part of the safety function are read by the device software. However, functions of the operating system may be used if the correctness of the read data are verified by the device software.

e) The test routines according to 4.6 shall be performed by the device software or hardware.

NOTE 1 If the state of switching outputs is monitored by the device software, functions of the operating system may be used both for driving and reading back the switching output.

NOTE 2 For digital data transmission between spatially separated components of apparatus the requirements of 4.5 apply. The device software verifies the transmitted information thus enabling the detection of side effects (e.g. corruption) caused by the operating system of the transmitter or receiver.

4.3.3 Software requirements

a) It shall be possible for the user to identify the installed software version, for example by marking on the installed memory component, in (if accessible) or on the apparatus or by showing it on the display during power up or on user command.

b) It shall not be possible for the user to modify the software function. It shall be impossible to change the program code under any operating conditions. Upgrades shall only be possible under the control of the manufacturer.

c) Parameter settings shall be checked for validity. Invalid inputs shall be rejected. An access barrier shall be provided against parameter changing by unauthorized persons, e.g. it may be integrated by an authorization code in the software or may be realized by a mechanical lock. Parameter settings shall be preserved after apparatus switch-off, after disconnection of the power supply and while passing through a special state.

   Parameters controlling the calibration of the apparatus shall not be updated before the calibration/adjustment routine is finished successfully. It shall be possible for the user to abort the calibration/adjustment routine.

   NOTE 1 If zero and span adjustment are carried out independently in separate routines, each parameter may be updated individually after the respective routine is finished successfully.

d) Control or status bits shall be explicitly set or re-set in each program cycle.

   NOTE 2 This may not be possible for all control and status bits (e.g. for latched alarms). Additional measures for detecting corruption are described in 4.8, requirement 4).

4.3.4 Requirements for software documentation

The software documentation shall include:

a) designation of the apparatus to which the software belongs;

b) unambiguous identification of program version;

c) if applicable, version the operating system;

d) if applicable, versions of libraries;

e) any software modification provided with the date of change and new identification data;

f) documentation of the software development process (modification included, if applicable) according to 4.3.5;

g) source code;

h) functional description;

i) software structure (e.g. flow chart, Nassi-Shneiderman diagram).

4.3.5 Requirements for the software development process

4.3.5.1 General

The software development shall be carried out according to the model described in Figure 1.

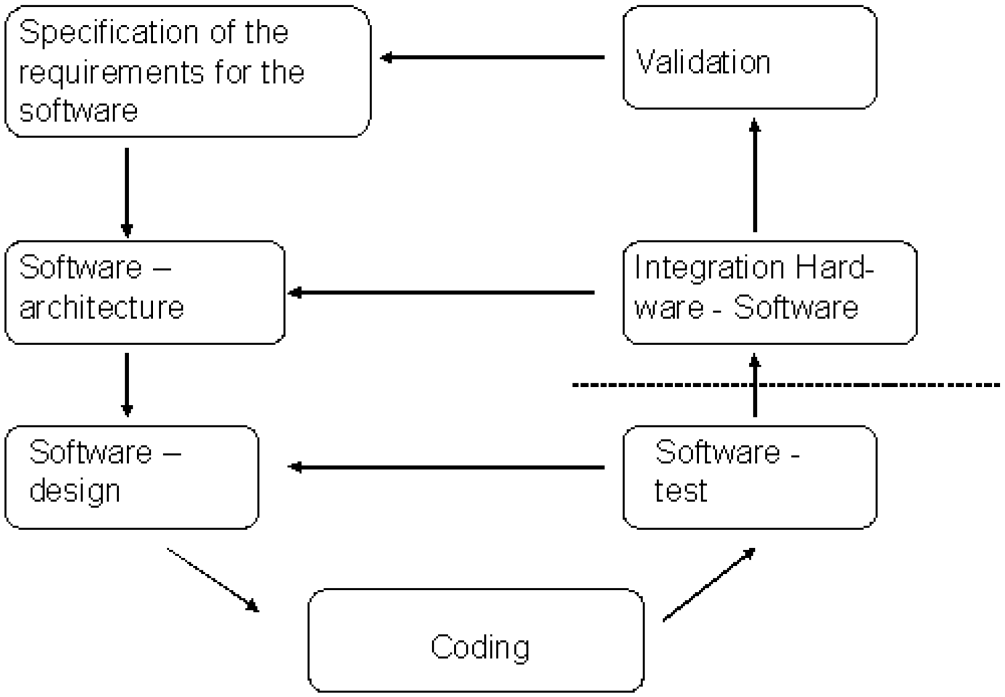

Figure 1 — Model of the software development process

It shall be ensured by suitable measures that

a) during development of the software

b) and for all modifications on the basis of an impact analysis

all applicable phases are processed and documented. For each software version, it shall be possible to identify all parts of the software (software-documentation included) with respect to their version and to identify the relationship between all parts unambiguously. That is, all parts of the software and all its documentation shall be held under configuration management.

NOTE 1 The application of these measures ensures in conjunction with the requirements for the software documentation according to 4.3.4 that the applicable requirements of EN 61508-3 to the configuration management of the software are fulfilled for the purpose of this European Standard.

The results of each phase of the software development process shall be verified for consistency with the input of the phase and for correctness as regards content. The results of each phase and the verification shall be reviewed and approved by a second person. The results of each phase, the results of the tests and the related verification shall be documented and held under configuration management.

This verification includes the requirement that the test plans developed in individual phases of the software development process shall be assessed with respect to their suitability and completeness.

NOTE 2 These tests and assessments include in conjunction with further regulations described in the following clauses the applicable requirements of EN 61508-3 for software verification.

NOTE 3 Configuration management can be achieved by use of a suitable tool or by specification of appropriate procedures.

Coding-guidelines shall be used in the coding phase. These shall

c) be used for the development of the entire software;

d) describe programming techniques to be used;

e) proscribe the use of unsafe language constructs;

f) specify procedures for source code documentation.

The documentation of each source code module shall contain at least the following:

g) legal entity (for example company, author(s));

h) intended use;

i) for each function/procedure, its inputs and outputs, their pre- and post-conditions, and their effect on global state.

j) history of versions.

4.3.5.2 Specification of the requirements for the software

The requirements for the software shall be specified for each interface, including: hardware components, human interfaces, communication interfaces. A concept for detection and handling of faults on all these hardware components and interfaces shall be defined.

NOTE 1 The interfaces to the hardware include also the interfaces to devices which are not part of the apparatus.

The requirements for the software shall be complete and unambiguous and shall be documented in sufficient detail in natural language. Where practical, graphical schemes, tables, mathematical formulas etc. may be used for the sake of precision.

It shall be possible to identify each requirement for the software unambiguously.

Each requirement for the software shall be traceable to a requirement for the apparatus.

A plan for validating the software shall be developed based on the specified requirements for the software. The objective of the validation is to demonstrate that all specified requirements for the software are satisfied.

NOTE 2 Parts of this validation will demonstrate that certain requirements of the metrological standards that apply to the functionality of the apparatus are fulfilled.

Validation shall be carried out with the apparatus and therefore also includes the interaction of hardware and software. Validation shall be carried out by means of a functional/black-box-test of the apparatus (see 4.3.5.8).

The validation plan shall include at least the following:

a) test methods and test cases for each specified requirement for the software;

b) environmental conditions;

c) tools (for example test gases);

d) pass / fail criteria.

4.3.5.3 Software architecture

4.3.5.3.1 Architecture

The software architecture shall be designed based on

a) hardware architecture;

b) specification of the requirements for the software (see 4.3.5.2).

The software architecture shall

c) define a structured and modular design;

d) ensure that software modules have a clearly defined interface to other modules;

e) specify each interaction between software and hardware;

f) define measures for detection and handling of hardware faults.

The design of the software architecture and the software design (see 4.3.5.4) shall be carried out in a structured manner. This includes a systematic approach including at least the following steps:

g) decomposition step by step of the software function into manageable software components;

h) assignment of data structures to the software components;

i) definition of the interfaces between the software components;

j) if applicable, selection of the operating system (see 4.3.1);

k) if applicable, selection of libraries (see 4.3.1).

The software architecture shall allow for tracing each requirement for the software from 4.3.5.2 to its implementation in the software design according to 4.3.5.4.

The hardware-software integration tests shall be specified based on the software architecture (see 4.3.5.7).

4.3.5.3.2 Tools and coding standards

Suitable, matching tools including languages, compilers, and, if used, tools for the configuration management and automatic testing tools shall be selected. The availability of the tools over the whole lifetime of the apparatus shall be considered.

The suitability of the tools for code generation (for example code generator, compiler) and of external or re-used software (for example libraries) shall be assessed. At least the following criteria shall be considered:

a) range of functions and performance;

b) operating experience;

c) updates, release notes;

d) error lists;

e) references;

f) publications related to the tool (for example tests or validation by a third party);

g) experience with similar products of the manufacturer;

h) market presence of the manufacturer.

NOTE 1 This assessment may be omitted if EN 61508 (or similar safety standard) certified tools are used.

Changing the version of the tools for code generation during the lifetime of the apparatus should be avoided because otherwise the suitability has to be re-assessed.

The programming language and the coding standards shall support measures to avoid systematic faults and foster predictable program execution. This can be achieved by applying the following criteria.

Requirements for the programming language (by using coding standards, if necessary):

i) suitability for the application;

j) complete, unambiguously defined or restricted to unambiguously defined properties;

k) contain features that facilitate the detection of programming mistakes;

l) block structure.

The language should be user- or problem-orientated rather than processor/platform machine-orientated. Widely used languages or their subsets are preferred to special purpose languages.

Low-level languages, in particular assembly languages, present problems due to their processor/platform machine-orientated nature. Therefore, assembly languages should only be used for tasks with low complexity. Any use of assembly language shall be justified explicitly in the software documentation.

The programming language and the use of coding standards, if necessary, shall support

m) restriction of access to data in specific software modules (encapsulation);

n) further measures for fault avoidance, for example avoidance of unsafe constructs.

If the programming language allows unsafe constructs, their use shall be avoided by definition of a subset. This subset shall be defined in coding standards.

NOTE 2 MISRA-C is an example of a language subset for the programming language C.

The use of the following unsafe constructs shall be avoided by the coding standards:

o) unconditional jumps excluding subroutine calls;

p) recursions;

q) dynamic variables or objects;

r) multiple entries or exits of loops;

s) multiple entries of subprograms or blocks;

t) implicit variable initialisation or declaration;

u) data of variable types (for example “void” in C);

v) equivalences of variables (for example “unions” in C), if write access occurs at more than one place of the program;

w) automatic type conversion.

Pointer shall only be used as far as absolutely necessary.

Subprograms and blocks shall have one exit only.

4.3.5.4 Software design

The software design shall be carried out in a structured manner (see 4.3.5.3). It shall be possible to demonstrate the implementation of each requirement for the software from 4.3.5.2.

The software design shall adhere to the following rules which shall be included in the coding guidelines:

a) decomposition of the software components into systems of software modules;

b) specification of the functionality of the software modules;

c) specification of data structures and assignment to the software modules; this specification shall be consistent with the functional requirements of the apparatus, complete and free of contradictions;

d) definition of unambiguous interfaces between the software modules;

e) design of the software modules;

f) specification of test methods and test cases for each software module (specification of module testing, see 4.3.5.6);

g) specification of test methods and test cases for the entire software (specification of software integration test, see 4.3.5.6).

The software design shall be carried out according to the following rules:

h) the software modules shall be decoupled as far as possible and all interactions are explicit;

i) suitable limitation of module size;

j) each interface of a software module shall only contain only those parameters which are necessary for its function;

k) compose the software module control flow using structured constructs, that is sequences, iterations and selection;

l) keep the number of possible paths through a software module small;

m) avoid complex branching;

n) avoid complicated calculations as basis for branching or loop conditions;

o) software modules shall usually communicate with other software modules via their interfaces - where global or common variables are used:

    1) they shall be well structured;

    2) they shall be easily identifiable;

    3) access shall be controlled;

    4) their use shall be justified in each instance;

    5) competing write- and read-access by parallel running processes shall be avoided;

p) multiple calls (for example by interrupts) of subprograms which are not re-entry capable shall be avoided.

4.3.5.5 Coding

The source code shall

a) be readable, understandable, and testable;

b) implement the design of the software modules (see 4.3.5.4);

c) satisfy the requirements of the coding standards (see 4.3.5.3.2);

d) implement each requirement for the software from 4.3.5.2.

It shall be verified for each software module by a tool-based static code analysis that the coding standards (see 4.3.5.3.2) are satisfied. Where a tool-based static code analysis is not sufficient or not possible, supplementary or alternative measures shall be taken (e.g. code review by a second person or code walk through).

4.3.5.6 Software test

The software test consists of software module tests and an integration test. These tests shall be carried out as functional/black-box tests (see Annex A).

Each software module shall be tested as specified during the software design (see 4.3.5.4). The software modules shall be combined to manageable integration units. The software integration test shall be carried out as specified during the software design (see 4.3.5.4). If appropriate, the software integration test and the hardware-software integration test according to 4.3.5.7 may be combined.

The specification of the module tests and the software integration test shall include

a) test cases and test data;

b) test methods;

c) test bed, tools, configuration and programs;

d) pass / fail criteria.

Software module tests contribute to the verification that the software modules satisfy all module specifications specified during the software design (see 4.3.5.4) completely. If it is not possible to cover all module specifications by functional/black-box tests according to Annex A additional software tests (e.g. white box testing) and/or code review shall be performed.

Software integration tests contribute to the verification that the software modules and software components/-subsystems interact correctly to perform their intended function.

Both for the software module test as well as the software integration test the test configuration, the test results, the assessment and, if applicable, corrective actions shall be documented. If software is modified as a result of the software integration tests the requirements in 4.3.5.1 shall be observed.

4.3.5.7 Hardware-software integration test

The hardware-software integration test shall be carried out as specified during the design of the software architecture (see 4.3.5.3). If appropriate, the software integration test according to 4.3.5.6 and the hardware-software integration test may be combined. The hardware-software integration test shall be carried out as functional/black-box test (see Annex A).

The specification of the hardware-software integration test shall include the following:

a) split of the integration into reasonable steps;

b) test cases and test data;

c) test methods;

d) test bed, tools, equipment, support software and configuration;

e) pass / fail criteria.

The test configuration, the test results, the assessment and, if applicable, corrective actions shall be documented. If hardware or software is modified as a result of the integration tests the requirements in 4.3.5.1 shall be observed.

4.3.5.8 Validation

Validation shall be carried out with the apparatus and therefore also includes the interaction of hardware and software. It is allowed to adopt results of the hardware-software integration test if these results were achieved with the hardware and software versions to be validated.

The validation shall be carried out as specified in the validation plan (see 4.3.5.2). The validation shall be carried out completely and demonstrate for the hardware and software versions to be validated that all specified requirements for the software are fulfilled. If validation results are used which were achieved with former versions of hardware or software it shall be verified by an impact analysis that the modifications have no impact on the validation results.

Tools and equipment used for software validation shall be suitable for purpose.

Validation shall be carried out as functional/black-box test (see Annex A).

Discrepancies between expected and actual results shall be analysed and a decision taken on whether to continue the validation for the time being, or to issue a change request immediately and return to an earlier phase of the software development process.

The documentation of the validation shall include the following:

a) a record of all validation activities which allows a chronology and identification of the validated versions of software and hardware for all activities;

b) the validated software function with respect to the validation plan and version of the validation plan;

c) tools and equipment used together with calibration data unless otherwise documented;

d) impact analysis concerning usability of validation results obtained with former versions of hardware and software, if applicable;

e) discrepancies between expected and actual results as well as the results of the analysis and the decision concerning further action;

f) assessment result “passed” or “failed” including justification.

4.3.5.9 Software modification

Corrections, enhancements or adaptations to the validated software shall be carried out in such a manner that the software safety is not affected.

A software modification request shall be prepared and released. The software modification request shall describe the proposed change and the reasons for change.

An impact analysis of the proposed software modification shall be carried out. Based on this analysis, decisions shall be taken

a) to which phase of the software development process it shall be returned;

b) the extent of the modifications to be made in this phase and each of those following.

The results of the impact analysis shall be documented.

On this basis a modification plan shall be developed. It shall include the following:

c) a detailed specification of the modification;

d) planning of the tests according to 4.3.5.6 and 4.3.5.7;

e) planning of the validation according to 4.3.5.8.

The tests according to d) shall include all modified subroutines and all subroutines which are affected by the modification. All original test cases, if applicable, and, if necessary, new test cases to be defined shall be carried out.

The modification shall be carried out as specified in the modification plan.

The requirements to the documentation according to 4.3.5.1 to 4.3.5.8 shall be fulfilled.

4.4 Hardware

Safety relevant components shall only be used within their specifications. For interconnection between components, cabling and other interface specifications shall be adhered to.

To store parameters and variables, which should be permanent even after switch-off or during a special state, storage parts shall be used in which the data content remains permanent when the supply voltage is removed. Where a back-up supply (e.g. battery, capacitor) is used for this purpose the test routine for the parameter memory (see 4.6) shall be able to detect a discharged supply.

It is not recommended to use a rechargeable battery.

4.5 Digital data transmission between components of apparatus

Digital data transmission between spatially separated components of equipment shall be reliable. The measures for ensuring reliable data transmission between spatially separated components shall take into account transmission errors, repetitions, deletion, insertion, resequencing, corruption, delay and masquerade. If transmission errors cause delays that are longer than one third of the response time t_{90} or time to alarm for alarm-only equipment, the equipment shall enter a defined special state.

In case of data transmission between components within a single enclosure a one-bit redundancy scheme shall be used (for example, parity checking) as the very minimum.

If the data transmission is used for more than one channel, e.g. bus connection or multiplex transmission, the correct assignment of the channels shall be monitored.

NOTE 1 Data transfer between a microcontroller and external A/D- or D/A-converters is not to be considered here. The respective requirements are described in 4.1.2 and 4.1.4.

NOTE 2 Data transfer between a microcontroller and external memory components is not to be considered here. The respective requirements are described in 4.6.

NOTE 3 Data transfer from a microcontroller to a display is not to be considered here. The respective requirements are described in 4.6.

Plug connections shall be protected against erroneous connection or disconnection.

If the non-ambiguity of the measured values of the whole apparatus at gas concentrations above the upper limit of the measuring range (e.g. when catalytic sensors are used) is affected by transmission errors the apparatus shall pass over to a defined latching special state.

4.6 Test routines

Computerized digital units shall incorporate test routines. On fault detection, the apparatus shall pass over to a defined special state. The tests except for tests b) and c) shall be done automatically, performed after switching on and repeated cyclically at least once within 24 h. The tests after switching on shall be completed before the special state “warm-up” is left.

It is permitted for fixed or transportable apparatus that the test after switching on can be skipped on user intervention for maintenance purposes (see 4.7 i)).

NOTE 1 Test routines for stuck-at faults of A/D-converters and multiplexers are not included because the failure rates of these components are usually very low. It is recommended that the manufacturer verifies that the failure rates of these components are negligible in comparison with the failure rates of the other digital components used in the apparatus.

The following minimum tests shall be performed by the apparatus:

a) supply voltage of digital units shall be monitored against under-range within time intervals of maximum ten times response time t_{90} or time to alarm for alarm only apparatus;

b) all visible and audible output functions shall be tested. The test shall be carried out automatically after starting operation. For portable apparatus which cannot be switched off and for transportable and fixed apparatus this test shall also be carried out on user request. It is permissible that the result is assessed by the user;

c) all safety relevant output signals shall be tested on user request. It is permissible that the result is assessed by the user;

NOTE 2 Visible or audible output functions according to b) are not considered here.

d) monitoring equipment with its own time base (e.g. watchdog) shall work independently and separately from the parts of the digital unit which perform the data processing. Triggering of the monitoring equipment shall be based on the program execution and shall not be solely time-related (e.g. based on a periodic timer interrupt);

NOTE 3 Independent operation is considered to be fulfilled if the operation of the monitoring equipment cannot be controlled by the digital unit which performs the data processing.

NOTE 4 Separate operation of the monitoring equipment is considered to be fulfilled if

- the voltage supply is separately connected to the power supply of the digital unit,
- negative affects (e.g. ESD, EMC) on the operation of the data processing unit are not likely to influence the operation of the monitoring equipment,
- malfunction of the data processing unit caused by thermal or electrical overload will not influence the operation of the monitoring equipment.

NOTE 5 Independent and separate operation will typically be ensured by using an external monitoring component.

Particular attention shall be paid on appropriate triggering conditions of the monitoring equipment in the program. It is recommended to monitor the execution of the relevant software modules in the correct order.

e) program (operating system included, if applicable) and parameter memory shall be monitored by procedures which allow the detection of all single bit errors and most of the two bit errors. All copies of program and/or parameters (e.g. in volatile memory) shall be included in the test routines. In the event of fault detection, parameters shall not be changed automatically. Restoring the valid values e.g. from redundant copies is allowed if the restored parameters are verified immediately afterwards;

Copies of constants in volatile memory at the time of program execution should be avoided. If such copies are used, it is recommended to monitor these copies by procedures which are used for monitoring parameter memory.

f) volatile memory shall be monitored by procedures that test the readability and writeability of the memory cells.

NOTE 6 Areas of the volatile memory which are not used for safety relevant data may be excluded from this test.

NOTE 7 Internal registers of the microprocessor, e.g. program counter, may be excluded from the test.

4.7 Instruction manual

The metrological standards contain requirements on the instruction manual. In addition, the following information shall be included:

a) instructions how switching outputs shall be wired and monitored for safe operation;

b) if provided, relevance of the alive signal or confidence signal for safety;

c) description of all special states including cause, signalling and termination;

d) description of all messages available to the user and methods for interrogation;

e) behaviour of displays, measuring outputs and all signal outputs at underscale or overscale;

f) minimum refresh rates of all safety relevant output signal(s);

g) all user changeable parameters and their valid ranges;

h) life time of data storage if a back-up battery is used for preserving the data content of parameter memory when the supply voltage is removed;

i) instruction for fixed or transportable apparatus, that the apparatus shall be re-started after end of maintenance work if the power-on self test has been skipped for this maintenance work;

j) description of the tests for the visible and audible output functions and the safety relevant output signals and instruction in which time intervals these tests shall be carried out;

k) instruction that after changing parameters by using an external device (e.g. PC), the user shall check the correctness of the parameter settings

   1) by checking the parameter settings at the gas detection apparatus; or alternatively

   2) by reading back the parameters from the gas detection apparatus and manually verifying the received values.

   NOTE The user is permitted to use pre-checking of the received parameters and marking of mis-matches by the external device.

If compliance with SIL 1 is claimed, the following information shall also be included:

l) description of the safety function(s);

m) PFD, λ_{DU} and λ_{DD}, proof-test interval T_1, assumed mean time to restoration (MTTR);

n) all special operating conditions which were the basis for the calculation of these figures;

o) content of the proof test;

p) recommended working life time;

q) recommended working life for consumables such as filters or chemical converters;

r) for aspirated apparatus (automatically aspirated apparatus excluded) instructions that the flow rate shall be monitored. Instructions shall be given that flow conditions (lower limit and upper limit if necessary) where the specified performance is not met, e.g. for measured value and response time, shall be detected and indicated as a fault;

s) specification of the maximum and minimum load conditions for the connection of devices to switching outputs. It shall be specified that the switching outputs shall be tested at least once per proof test interval;

t) Requirement that failure of an active element (e.g. cooling or heating) used for conditioning of measured gas of aspirated apparatus shall be detected and indicated as a fault.

4.8 Additional requirements for compliance with SIL 1

This clause shall be applied to fixed and transportable apparatus where compliance with safety integrity level 1 (SIL 1) according to EN 61508 series is claimed. It can also be applied to portable apparatus which are able to perform an automatic executive action.

This clause shall be applied for every safety function.

The following additional requirements shall be fulfilled:

1) Switching outputs:

   In the case of relays the possibility of a short circuit between coil and contact shall be excluded by constructional means, e.g. by sealing.

   In the case of optocouplers the possibility of a short circuit between its sending and receiving part shall be excluded by constructional means, e.g. by sealing.

   The switching output shall be energized in normal operation mode or the input circuit (e.g. relay coil) of the switching output shall be monitored by a procedure which detects a failure of the input circuit within 24 h.

2) Internal power supply:

   In addition to monitoring of the supply voltage of digital units (see 4.6 a)) all further regulated voltages of safety relevant components shall be monitored in time intervals of maximum ten times response time t_{90} or time to alarm for alarm only apparatus. In case of fault detection the apparatus shall switch to a defined special state.

3) Control and status bits:

   Requirement 4.3.3 d) is replaced by:

   Control or status bits shall be explicitly set or re-set in each program cycle. If this is not possible (e.g. for latched alarms) the state shall at least be verified against a copy or other means of detecting corruption.

4) Monitoring of flow rate:

   Automatically aspirated apparatus shall monitor the flow rate. Flow conditions (lower limit and upper limit if necessary) where the specified performance is not met, e.g. for measured value and response time, shall be indicated as a fault.

Regarding the software development process, the following additional requirements to 4.3 shall be fulfilled:

5) Offline numerical analysis:

   Add at the end of 4.3.5.5:

   Where the measurement computation is complex, that is, where more than simple calculation (e.g. calibration in form of a linear equation or averaging) is required, then a numerical analysis to show the stability and accuracy of the implementation of the algorithms shall be performed.

6) Structural test coverage (entry points) 100 %:

Paragraph 4 in 4.3.5.6 replaced by:

Software module tests contribute to the verification that the software modules satisfy all module specifications specified during the software design (see 4.3.5.4) completely. If it is not possible to cover all module specifications by functional/black-box tests according to Annex A additional software tests (e.g. white box testing) and/or code review shall be performed. In addition, it shall be ensured that all entry points to functions and subroutines within a module are called at least once. Where 100 % coverage cannot be achieved, an appropriate explanation shall be given and the evidence of coverage shall be achieved by review.

If a gas detection apparatus complies with the metrological standards and with the requirements of 4.1, 4.2, 4.4, 4.5 and 4.6 a safe failure fraction (SFF) of 60 % to 90 % is assumed to be achieved.

NOTE This SFF is sufficient for complex apparatus with a hardware fault tolerance (HFT) of zero to comply with SIL 1.

The following figures shall be calculated for the entire apparatus:

a) failure rates λ_{DU} and λ_{DD};

b) average probability of failure on demand PFD:

$$PFD_{avg} = \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD}MTTR$$

where

λ_{DU}	is the dangerous undetected failure rate;
λ_{DD}	is the dangerous detected failure rate;
T_1	is the specified proof test interval;
MTTR	is the assumed mean time to restoration.

To determine the hardware failure rates for sensors, the gas detection apparatus manufacturer requires sufficient information about the failure modes of the sensing elements. Failure rates for sensing elements shall be estimated on the basis of:

- the failure modes for the specific measuring principle (information can be found in Annex D of EN 50402:2017),
- additional failure information by the manufacturer of the sensing element, if any,
- failure rates based on the experiences of the apparatus manufacturer related to relevant fields of application for their apparatus.

5 Test of the digital unit

5.1 General

The testing of the digital units is part of the testing of the apparatus for compliance with the performance requirements. It is divided into two phases. In the first phase the functional concept of the digital unit is inspected with regard to meeting the requirements to the design and to the software development process (Clause 4) within the framework of the entire apparatus. The second phase comprises a performance test of the digital units. It shall detect errors that can occur when transferring the design concept into hard- and software.

Because of multiple modes of realization and application of digital units the testing scheme shall be adapted to the conditions of each apparatus.

5.2 Verification of functional concept

Functional concept analysis and evaluation depend on the documentation from the manufacturer. The verification shall be performed by using the following list.

a) Functional description of the digital unit which is preferably structured like Clause 4:

   1) measuring sequence (including all possible variations);

   2) handling of range violations of input, internal and output data (see 4.1.4);

   3) estimation of numerical errors according to 4.1.3;

   4) possible special states (see 4.1.5);

   5) parameters and their permitted adjustment range;

   6) representation of measured values and messages;

   7) generation of alarms and signals;

   8) extent and realization of remote data transmission;

   9) extent and realization of test routines.

b) Hardware description:

   1) design of the digital unit (circuit diagrams, bill of materials (parts lists), relevant data sheets);

   2) block functional description of the digital unit;

   3) resolution, errors and input/output ranges of A/D- or D/A-interfaces;

   4) specification of interfaces between functional parts (with description of the coding procedure used for the digital data transmission).

c) Software documentation:

   1) according to 4.3.4.

   NOTE The software documentation is only for the use of the test laboratory. All information is confidential and is the property of the manufacturer.

The design of the digital units and the software development process shall conform to the requirements of Clause 4.

5.3 Performance test

The apparatus shall be operated during the performance test in such a manner that, starting from the measuring state, it enters all special states.

The following operation states shall be performed if applicable:

a) four measured values distributed over the measuring range;

b) measuring range under- and overflow;

c) special states if they can be entered without destruction of the hardware or modification of the software;

d) activation of every message;

e) test routines if they can be tested without destruction of the hardware or modification of the software;

f) change of parameters.

Operation states a) and b) shall be performed for a selection of measuring ranges, including the minimum and maximum range.

The tests are executed under the normal conditions for test given in the applicable metrological standards.

The function of the digital unit shall be identical to the function described in the instruction manual and the documentation according to 5.2.

Annex A
(normative)

Hardware-software integration test

A.1 Functional testing/Black-box testing

Aim:

To reveal faults which were brought in during the software development process up to the phase coding, by testing the dynamic behaviour under real functional conditions. To reveal incomplete specification or failure to comply with the specification and to assess utility and robustness.

Description:

The functions of the software, its components or modules are executed in a specified environment with specified test data which are derived systematically from the respective specification. This exposes the behaviour of the software, its components or modules and permits a comparison with the respective specification. Information about the internal structure of the software is not used for testing. The outputs and the behaviour are monitored and compared with the respective specification. Deviations from the specification and indications of an incomplete specification are documented. Suitable test data shall be defined so that all functions required in the respective specification are tested. An equivalence class test with boundary value analysis shall be performed.

A.2 Equivalence class test with boundary value analysis

Aim:

To test the software adequately using a manageable amount of test data. The test data set is obtained by suitable dividing the input data space into a limited number of equivalence classes. To detect software errors occurring at boundary values.

Description:

The input data space is subdivided into specific input value ranges (equivalence classes) with the aid of the specification.

This subdivision can be made input orientated or output orientated. For input orientated division all values of an equivalence class are treated in the same way; for output orientated division all values of an equivalence class lead to the same functional result.

NOTE 1 Example for an input orientated division: 1 is added to numbers between 1 and 9, 2 is added to numbers between 10 and 99, 3 is added to numbers between 100 and 999, a fault message is released for numbers higher than 999. Each number range represents an equivalence class, all numbers of one range are treated in the same way.

NOTE 2 Example for an output orientated division: Triples of numbers designate the lengths of the sides of a triangle. The triples are used to determine whether the triangle is equilateral, isosceles or nothing of these. Triples with three identical elements lead to the same result (equilateral triangle) and form the equivalence class “equilateral triangle”; triple with two identical elements form the equivalence class “isosceles triangle” etc.

Test cases are selected with the aim of covering all the equivalence classes previously specified. At least one test case is taken from each equivalence class. For each equivalence class the following test cases shall be formed:

a) data from permissible ranges;

b) data from inadmissible ranges;

c) data from the range limits;

d) extreme values;

e) and combinations of the above classes, where reasonable.

Other criteria can be effective in order to select test cases in the various test activities (software test, hardware-software integration test).

The tests at the range limits of the equivalence classes check that the boundaries in the input domain of the specification coincide with those in the program. The use of the value zero, in a direct as well as in an indirect use, is often error-prone and demands special attention:

f) zero divisor;

g) blank ASCII characters;

h) empty stack or list element;

i) full matrix;

j) zero table entry.

Normally the boundaries for input have a direct correspondence to the boundaries for the output range. Test cases shall be defined to force the output to its limit values. It shall also be considered whether it is possible to specify a test case which causes the output to exceed the specified boundary values. If the output is a sequence of data, for example a printed table, special attention shall be paid to the first and the last element and to lists containing none, one or two elements.

Annex ZY
(normative)

Significant changes between this European Standard and EN 50271:2010

This European Standard supersedes EN 50271:2010.

The significant changes with respect to EN 50271:2010 are as listed below.

	Type		
	Minor and editorial changes	**Extension**	**Substantial change regarding ESR´s [a]**
Modification of the introduction for better alignment with EN 50402:2017	X		
Modification of the scope (Update of references to standards and re-wording of text related to SIL 1)	X		
Normative references (new editions of cited standards)	X		
Definitions re-formulated for better alignment with EN 50402:2017 and added definition 3.15 for clarity	X		
4.1.2, 4.1.3, 4.1.4: Text re-worded for clarity	X		
New 4.1.5.1 General: Clause added for clarity	X		
4.1.5.2: Text re-worded for clarity and better compatibility with metrological standards	X		
4.2.3: Text added for clarity	X		
4.3.1: Text added and re-worded for clarity and correction of an error	X	X	
4.3.3: NOTE added for clarity	X		
4.3.5.1: Text re-worded for clarity and correction of an error	X		
4.3.5.2: Redundant text deleted and text re-worded for clarity	X		

4.3.5.3.1: Text re-worded for clarity	X		
4.3.5.3.2: Implicit requirement made explicit by adding w); example added	X		
4.3.5.4: Text re-worded for clarity and requirement o2) formulated in a more general way.	X		
4.3.5.5: Text re-worded for clarity	X		
4.3.5.6: Text re-worded for clarity	X		
4.6: Text re-worded for clarity	X		
4.7: Text of a) re-worded and NOTE added to k) for clarity	X		
4.7: Requirements are extended for compatibility with SIL 1 requirements of EN 50402:2017		X	
4.8: Requirements are extended for compatibility with SIL 1 requirements of EN 50402:2017		X	
[a] ESR = Essential Health and Safety Requirements (Annex II of Directive 2014/34/EU)			

General conclusion on the change of the State of the Art by this European Standard

CLC/SC 31-9 as the responsible body has concluded that this new edition contains no substantial changes regarding the ESRs.

Annex ZZ
(informative)

Relationship between this European standard and the essential requirements of Directive 2014/34/EU aimed to be covered

This European Standard has been prepared under a Commission's standardization request "M/BC/CEN/92/46" to provide one voluntary means of conforming to Essential Requirements of 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (recast).

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 II of Directive 2014/34/EU

Essential Requirements of Directive2014/34/EU	Clause(s) / subclause(s) of this EN	Remarks / Notes
1.5.5 - 1.5.7	whole standard except Clause 4.3	when used in conjunction with EN 60079–29–1, EN 50104 or EN 60079–29–4
1.5.8	4.1.2 (parts), 4.1.4 (parts), 4.3	
NOTETo confer a presumption of conformity with the relevant essential requirements of Directive 2014/34/EU, this standard has to be applied together at least with one of those standards as specified in Remarks/Note Column.		

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.

Bibliography

EN 45544-1, *Workplace atmospheres – Electrical apparatus used for the direct detection and direct concentration measurement of toxic gases and vapours – Part 1: General requirements and test methods*

EN 45544-2, *Workplace atmospheres – Electrical apparatus used for the direct detection and direct concentration measurement of toxic gases and vapours – Part 2: Performance requirements for apparatus used for exposure measurement*

EN 45544-3, *Workplace atmospheres – Electrical apparatus used for the direct detection and direct concentration measurement of toxic gases and vapours – Part 3: Performance requirements for apparatus used for general gas detection*

EN 45544-4, *Workplace atmospheres – Electrical apparatus used for the direct detection and direct concentration measurement of toxic gases and vapours – Part 4: Guide for selection, installation, use and maintenance*

EN 50104, *Electrical apparatus for the detection and measurement of oxygen - Performance requirements and test methods*

EN 50194-1, *Electrical apparatus for the detection of combustible gases in domestic premises - Part 1: Test methods and performance requirements*

EN 50194-2, *Electrical apparatus for the detection of combustible gases in domestic premises - Part 2: Electrical apparatus for continuous operation in a fixed installation in recreational vehicles and similar premises - Additional test methods and performance requirements*

EN 50291-1, *Electrical apparatus for the detection of carbon monoxide in domestic premises - Part 1: Test methods and performance requirements*

EN 50291-2, *Electrical apparatus for the detection of carbon monoxide in domestic premises - Part 2: Electrical apparatus for continuous operation in a fixed installation in recreational vehicles and similar premises including recreational craft - Additional test methods and performance requirements*

EN 60079-29-2, *Explosive atmospheres – Part 29-2: Gas detectors – Selection, installation, use and maintenance of detectors for flammable gases and oxygen (IEC 60079-29-2)*

EN 60079-29-4, *Explosive atmospheres - Part 29-4: Gas detectors - Performance requirements of open path detectors for flammable gases*

This page is intentionally left blank

National Standards Authority of Ireland

NSAI is the state standardization body set up under the National Standards Authority of Ireland Act 1996 to publish Irish Standards.

Revisions

Irish Standards are updated by amendment or revisions from time to time. Users of Irish Standards should make sure that they possess the latest versions.

NSAI's **Tailored updating service** is designed to meet your precise needs and is therefore the most efficient and cost-effective way of keeping ahead. For more details on the tailored updating service see:

Standards.ie
Tel.: +353 1 857 6730/1

Buying standards

NSAI and International publications can be accessed:

- at standards.ie
- by tel: +353 1 857 6730/1 or
- email: info@standards.ie.

Feedback on Standards

NSAI welcomes any comments on standards whether proposing an amendment, correcting an error or identifying an ambiguity. Please use the "About NSAI" and then "Contact us" buttons on the **NSAI.ie** home page to explain your comment.

Participation in developing Standards

NSAI Standards, whether of National, European or International origin, are drawn up by panels of experts. Persons with expert knowledge in any field where standardization work is taking place and who are interested in contributing to the work of the panels are welcome to make themselves known to NSAI. Please note that conditions apply. Click on the "Get involved in Standards Development" button in **NSAI.ie**

This page has been left intentionally blank.