BS EN 60079-29-3:2014

BSI Standards Publication

Explosive atmospheres

Part 29-3: Gas detectors - Guidance on functional safety of fixed gas detection systems

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 60079-29-3:2014. It is identical to IEC 60079-29-3:2014.

The UK participation in its preparation was entrusted by Technical Committee EXL/31, Equipment for explosive atmospheres, to Subcommittee EXL/31/3, Codes of practice.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

ISBN 978 0 580 76167 6
ICS 29.260.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2014.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60079-29-3

June 2014

ICS 29.260.20

English Version

Explosive atmospheres - Part 29-3: Gas detectors - Guidance on functional safety of fixed gas detection systems (IEC 60079-29-3:2014)

Atmosphères explosives - Partie 29-3: Détecteurs de gaz - Recommandations relatives à la sécurité fonctionnelle des systèmes fixes de détection de gaz (CEI 60079-29-3:2014)

Explosionsfähige Atmosphäre - Teil 29-3: Gasmessgeräte - Leitfaden zur funktionalen Sicherheit von ortsfesten Gaswarnsystemen (IEC 60079-29-3:2014)

This European Standard was approved by CENELEC on 2014-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 60079-29-3:2014 E

Foreword

The text of document 31/1105A/FDIS, future edition 1 of IEC 60079-29-3, prepared by IEC TC 31, Equipment for explosive atmospheres, was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 60079-29-3:2014.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-02-01
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2017-05-01

This part of IEC 60079-29 is to be used in conjunction with the following standards:

– IEC 60079-0, Explosive atmospheres – Part 0: Equipment – General requirements
– IEC 60079-29-1, Explosive atmospheres – Part 29-1: Gas detectors – Performance requirements of detectors for flammable gases
– IEC 60079-29-2, Explosive atmospheres – Part 29-2: Gas detectors – Selection, installation, use and maintenance of detectors for flammable gases and oxygen
– IEC 60079-29-4, Explosive atmospheres – Part 29-4: Gas detectors – Performance requirements of open path detectors for flammable gases

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

Endorsement notice

The text of the International Standard IEC 60079-29-3:2014 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60079-1	NOTE	Harmonised as EN 60079-10-1.
IEC 61511-1	NOTE	Harmonised as EN 61511-1.
IEC 61511-2	NOTE	Harmonised as EN 61511-2.
IEC 61511-3	NOTE	Harmonised as EN 61511-3.

Annex ZA
(normative)
Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu

Publication	Year	Title	EN/HD	Year
IEC 60079-29-1 (mod)	-	Explosive atmospheres -- Part 29-1: Gas detectors - Performance requirements of detectors for flammable gases	EN 60079-29-1	-
			+AA	
IEC 60079-29-2	2007	Explosive atmospheres -- Part 29-2: Gas detectors - Selection, installation, use and maintenance of detectors for flammable gases and oxygen	EN 60079-29-2	2007
			+EN 60079-29-2:2007/corrigendum Dec. 2007	2007
IEC 60079-29-4 (mod)	-	Explosive atmospheres -- Part 29-4: Gas detectors - Performance requirements of open path detectors for flammable gases	EN 60079-29-4	-
			+AA	
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series

IEC 60079-29-3

Edition 1.0 2014-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Explosive atmospheres –
Part 29-3: Gas detectors – Guidance on functional safety of fixed gas detection systems

Atmosphères explosives –
Partie 29-3: Détecteurs de gaz – Recommandations relatives à la sécurité fonctionnelle des systèmes fixes de détection de gaz

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX X

ICS 29.260.20 ISBN 978-2-8322-1496-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

EXPLOSIVE ATMOSPHERES –

Part 29-3: Gas detectors – Guidance on functional safety of fixed gas detection systems

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 60079-29-3 has been prepared by IEC technical committee 31: Equipment for explosive atmospheres.

This part of IEC 60079-29 is to be used in conjunction with the following standards:

– IEC 60079-0, *Explosive atmospheres – Part 0: Equipment – General requirements*
– IEC 60079-29-1, *Explosive atmospheres – Part 29-1: Gas detectors – Performance requirements of detectors for flammable gases*
– IEC 60079-29-2, *Explosive atmospheres – Part 29-2: Gas detectors – Selection, installation, use and maintenance of detectors for flammable gases and oxygen*
– IEC 60079-29-4, *Explosive atmospheres – Part 29-4: Gas detectors – Performance requirements of open path detectors for flammable gases*

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

FDIS	Report on voting
31/1105A/FDIS	31/1117/RVD

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

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

A list of all parts of the IEC 60079 series, under the general title: *Explosive atmospheres*, 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

Fixed gas detection systems have been used for many years to perform safety instrumented functions. Like any instrumented system, a fixed gas detection system commonly comprises of a single or multiple gas detector input(s), a control unit and a single or multiple final element(s) or output(s). Additional peripheral equipment may be incorporated into a fixed gas detection system e.g. a gas sampling system or a gas conditioning system. If a fixed gas detection system, including any relevant peripheral equipment is to be effectively used for safety instrumented functions, it is essential that the total system achieves certain minimum standards and performance levels.

It is important to understand that the number of sensing points and their appropriate location, their redundancy, the management of regular maintenance, specifically response checking or calibration, and other gas detection specific features (such as design of gas sampling systems) are all likely to have a far greater effect on the integrity of the overall Safety Instrumented System (SIS) than the required Safety Integrity Level (SIL) or SIL-capability of any of the individual functional units. This, however, does not exclude the requirement for each Safety Instrumented Function (SIF) to have a stand-alone functional integrity.

This international standard addresses the minimum standards and performance levels of a fixed gas detection system which is based on the use of electrical, electronic or programmable electronic systems (E/E/PES) for any application where there is either a risk reduction target stated or if the gas detection system is used as an additional safe guarding system.

This international standard does not apply to portable gas detectors or fixed gas detection systems when there is no risk reduction target stated. However, this standard could be used as a best practice document for such devices or systems.

The expression 'gas detection system' within this international standard is generic and applies to standalone fixed gas detectors, which might have their own internal alarm trip levels and switching outputs up to complex standalone fixed gas detection systems (Annex A – Typical Applications).

This international standard takes into consideration the possible complexity of the supply chain which a gas detection manufacturer, seller or system integrator might encounter which includes, but is not limited to:

- the use of standalone gas detectors which are integrated into an overall safety system by a gas detection equipment manufacturer, seller or system integrator (or equivalent)
- the design and use of fixed gas detection sub-systems, including any associated and/or peripheral gas detection equipment which are integrated into an overall safety system by a gas detection equipment manufacturer, seller or system integrator (or equivalent)
- the design and use of a complete fixed gas detection system, including associated and/or peripheral gas detection equipment which is the overall safety system

NOTE 1 IEC 61508 Parts 1, 2 and 3 cover the design of the stand-alone gas detector, control unit or final element. Guidance on the design of peripheral equipment is included within this international standard.

Before this international standard can be applied, it is important to understand and categorise the application of the fixed gas detection system. The three main applications are:

- as a prevention system – the total system or an individual instrumented control loop has a safety function and safety integrity clearly defined.
- as a mitigation system – the total system or an individual instrumented control loop has a safety function and safety integrity clearly defined.
- as an additional safe guarding system – this covers those fixed gas detection systems or individual instrumented control loops which operate in parallel (secondary) to an

instrumented safety system, where the demand on the fixed gas detection system or individual instrumented control loop is only when the primary instrumented safety system fails or another layer of protection fails.

Under no circumstances should the use of an additional safeguarding gas detection system contribute to the Hardware Fault Tolerance (HFT) declaration for the instrumented safety system.

A fixed gas detection system, as shown in Figure 1, may operate several times per year subject to the application, therefore this international standard accepts that the demand rate associated with 'on demand' (low demand) should be specified in the safety requirements (e.g. a reference could be "> 1/yr but <10/yr").

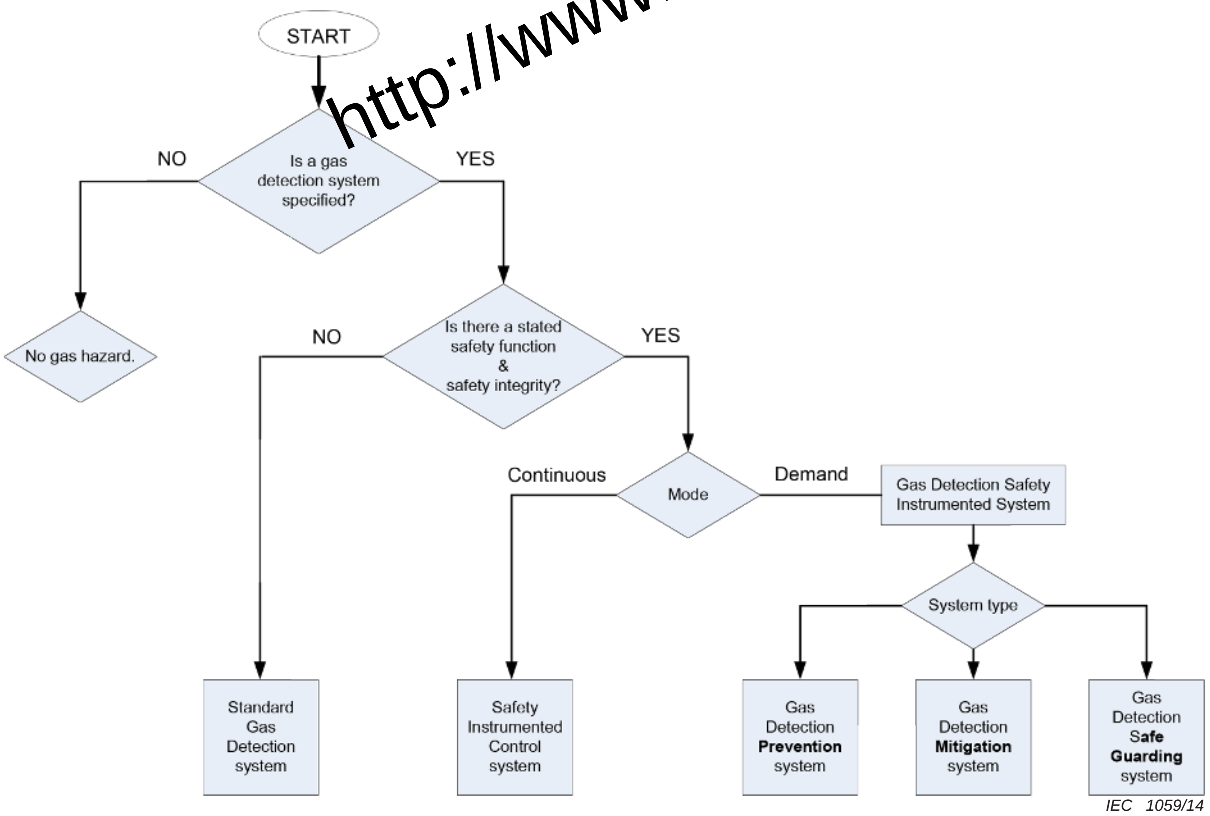


Figure 1 – Gas Detection System Architecture

To assist with the possible complexity and unique requirements associated with fixed gas detection systems, a fixed gas detection system may be broken down into functional units. Each functional unit can vary in complexity; a functional unit may be a simple gas detector or a combination of components which form peripheral equipment. Each functional unit is independently assessed against this international standard and/or IEC 61508 during the initial design phase of the functional unit, thus allowing safety data to be contributed to a functional unit.

NOTE 2 Basic elements of a sub-system/system (e.g. a gas detector, logic controller/solver, etc.) are designed as a product in compliance with IEC 61508 Parts 1, 2 and 3.

Each functional unit is then assembled in line with this international standard to deliver a complete fixed gas detection system. It is not necessary to re-assess individual functional units when they are used in a different configuration – it is only necessary to evaluate the combination of functional units.

This international standard is based on the safety lifecycle model detailed in IEC 61508, but adds additional and supportive information to assist with particular phases of this typical safety lifecycle.

This international standard specifies those requirements under 'Functional Safety Management' which all persons or companies who are involved in the supply chain of a fixed gas detection system should comply with.

NOTE 3 Functional Safety Management applies to all stages of the safety lifecycle irrespective of the product, subsystem, system supply or service being supplied.

For this document, the SIL capability excludes consideration of gas detection coverage or the transport of gas or vapour to the measuring point – IEC 60079-29-2 is pertinent to these two subjects.

Table 1 gives a broad suggestion as to the most relevant clauses to the typical tasks to be performed.

Table 1 – Typical Job Descriptions and Most Relevant Clauses

Applies to	Definitions	Conformance to this International standard	Gas detection unique features	Functional safety management	General requirements	Gas detection unique requirements	Alternative control units (logic solvers)	Factory acceptance testing	Installation and commissioning	System validation (SAT)	Operation and maintenance	System modification	System de-commissioning	Documentation
Clause	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Consultant		+++		+++										
Contractor		+++		+++										
Vendor		+++		+++										
System Integrator		+++		+++										
Manufacturer		+++		+++										
NOTE Each category above will have personnel in several of the categories below.														
General management	+	+	+		+	+	+	+	+	+	++	++	+	+
Design engineering / management	+++	+	+++		+++	+++	+++	+	+	+	++	+++	++	++
System engineer / management	+++	+	+++		+++	+++	+++	+++	++	++	+	+++	++	++
Installation engineering / management	++	+	++		+	++	+	+	+++	++	+	++	++	++
Commissioning engineer / management	++	+	++		++	++	+	+	+++	++	+	++	++	++
Service engineer / management	++	+	++		++	++	+	+	++	++	+++	+++	+++	++
Quality engineer / management	++	+	+++		+++	+++	+	+++	++	+++	+	++	+	+++
Training officers	+++	+	+++		+++	+++	++	+	+	+	+++	+	+	++
Operation & maintenance	+	+	++		+	++	+	++	+	+++	+++	+++	+++	+++

"+++" Most appropriate "++" Advisable "+" Useful

The end-user, regulator and certification authorities need to be familiar with the entire family of IEC 61508 standards.

NOTE See Annex B for guidance on the life cycle of gas detection.

EXPLOSIVE ATMOSPHERES –

Part 29-3: Gas detectors – Guidance on functional safety of fixed gas detection systems

1 Scope

This International standard gives guidance for the design and implementation of a fixed gas detection system, including associated and/or peripheral gas detection equipment, for the detection of flammable gases/vapours and Oxygen when used in a safety-related application in accordance with IEC 61508 and IEC 61511. This International standard also applies to the detection of toxic gases.

Other parts of this international standard and pertinent local, national and international standards separately specify the performance requirements of a gas detector and a gas detection control unit (logic solver). These standards are commonly known as Metrological Performance Standards and are concerned with the accuracy of the measured value, the overall system performance, but not the device or system integrity with respect to the safety function. This international standard applies to the integrity of the safety function.

NOTE In certain jurisdictions, it can be a requirement for a Certification Body to certify the performance of equipment for the measurement of flammable gases, vapours, toxic gases and/or Oxygen used in life safety applications.

This international standard sets out safety-related considerations of fixed gas detection systems, including associated and/or peripheral gas detection equipment in terms of the framework and philosophy of IEC 61508, and introduces the particular requirements demanded by a fixed gas detection system as shown in Figure 2.

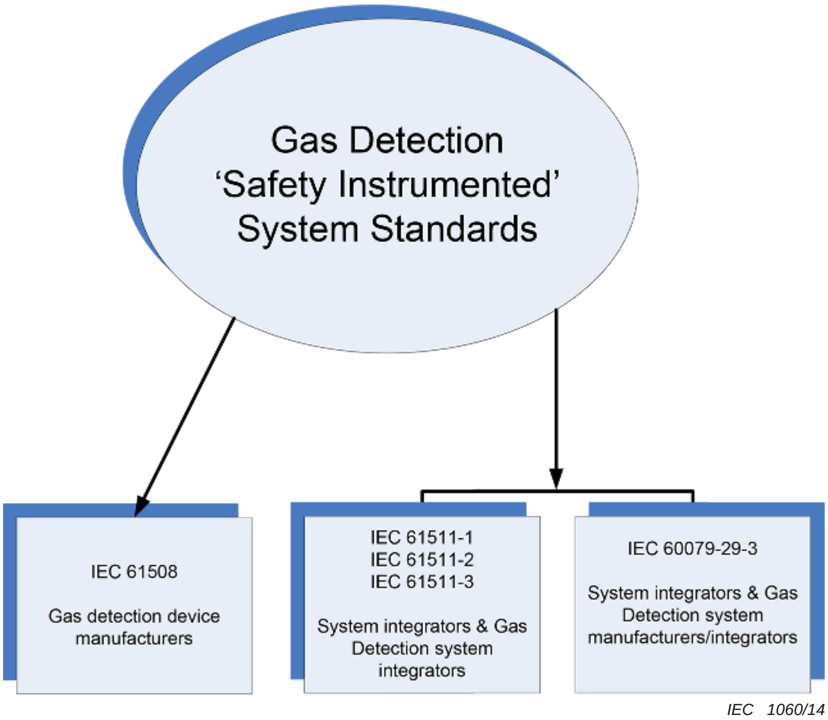


Figure 2 – Related Safety Instrumented System Standards

This international standard does not consider the Safety Integrity Level SIL 4. SIL 4 is assumed to be unrealistic to be achieved for gas detection systems.

NOTE 3 It is rare for any risk study to determine a Safety Integrity higher than SIL 2 for a fixed gas detection system.

This international standard is applicable for fixed gas detection systems, which might consist of the following hardware functional units

- Gas sensor/transmitter
- Gas detection control unit (logic solver)
- Gas sampling (single and multiplexed streams)
- Gas conditioning
- Automatic gas calibration and adjustment
- Output module (if not part of the control unit)

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

IEC 60079-29-2:2007, *Explosive atmospheres – Part 29-2: Gas detectors – Selection, installation, use and maintenance of detectors for flammable gases and oxygen*

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

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
additional safe guarding system
fixed gas detection system or individual instrumented control loops which operate in parallel (secondary) to an instrumented safety system, where the demand on the fixed gas detection system or individual instrumented control loop is only when the primary instrumented safety system fails or another layer of protection fails

3.2
associated gas detection equipment
equipment additional to the gas detection equipment covered by IEC 60079-29-1 or IEC 60079-29-4 which is part of the overall fixed gas detection system and is essential with respect to the safety function

Note 1 to entry: Examples of associated gas detection equipment are gas sampling or gas multiplexing.

3.3
dangerous failure
failure which has the potential to put the safety-related system in a hazardous or fail-to-function state

Note 1 to entry: Whether or not the potential is realised can depend on the channel architecture of the system; in systems with redundant/multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

Note 2 to entry: An example of a dangerous failure is the loss of a sensing head.

3.4
fail safe mode
mode of output signal where the normal operation is the energised mode.

Note 1 to entry: In the case of loss of power supply the output will be de-energised and the signal is active.

3.5
fault signal
audible, visible or other type of output, different from the alarm signal, permitting, directly or indirectly, a warning or indication that the equipment is not working satisfactorily

3.6
functional unit
entity of hardware or software, or both, capable of accomplishing a specified purpose which may consist of several elements

3.7
hardware module
entity of hardware capable of accomplishing a specified purpose e.g. a transmitter or control unit

3.8
measuring point
location of a gas detector

3.9
peripheral equipment
equipment which is part of the overall fixed gas detection system but is usually non-essential with respect to the safety function

Note 1 to entry: Data storage is an example independent from the safety function.

3.10
proof test
periodic test performed to detect hidden failures in a safety-related system so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition

3.11
safe failure
failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state

Note 1 to entry: An example of a safe failure is a fault in an EMC filtering circuit which has no influence in normal operation but may cause a spurious alarm when EMC disturbances are present.

3.12
safe state
state of the equipment under control (EUC) when safety is achieved

Note 1 to entry: In going from a potentially hazardous condition to the final safe state, the EUC may have to go through a number of intermediate safe states. For some situations, a safe state exists only so long as the EUC is continuously controlled. Such continuous control can be for a short or an indefinite period of time.

3.13
sample line
dedicated pipe or tube which connects a sample point to a gas detector within a point to point or multi-stream sampling system

3.14
sample point
end of a sample line where the sampled gas is taken from

Note 1 to entry: A sample point (hardware) normally comprises a physical housing containing a particle filter or equivalent.

3.15
SIL-capability
characteristic of functional units that comply with the requirements of IEC 61508-2 and IEC 61508-3 suitable for use in functions which are allocated a SIL 1, 2 or 3 respectively

3.16
special state
state of the equipment other than that in which monitoring of gas concentration takes place, for example warm-up, calibration mode or fault condition

4 Requirements

4.1 General

It should be ensured that each of the requirements outlined in Clauses 5 through 16 has been satisfied to the defined criteria and therefore the clause objective(s) have been met.

4.2 Demand rate

A fixed gas detection system may operate several times per year subject to the application, therefore this international standard accepts that the demand rate associated with ‘on demand’ (low demand) should be specified in the safety requirements (e.g. a reference could be “> 1/yr but <10/yr”).

Proof test intervals for low demand mode are determined with the assumption that the demand rate is maximum 1 per year.

If the specified demand rate is higher than 1 per year by factor “X” the proof test interval shall be reduced by the factor “X”.

5 Gas detection unique features

5.1 Objective

The objective of Clause 5 is to identify unique features which apply to fixed gas detection systems with respect to other sensing elements, instrumented control systems and actuators.

5.2 Features

5.2.1 General

Fixed gas detection systems differ from standard instrumented systems in many ways. During the design and engineering phase of any fixed gas detection system it is necessary to understand the features and/or unique demands associated with gas detection. 5.2.2 to 5.2.17 detail those main differences.

NOTE See IEC 60079-29-2 for guidance on selection, installation, use and maintenance of detectors for flammable gases and oxygen. This document gives additional information for many of the subclauses in Clause 8 of IEC 60079-29-2:2007.

5.2.2 Sensor location

Gas detection systems are reliant upon a transport mechanism to move the gas leak/vapour to the sensing element, unlike process safety devices such as pressure and temperature sensors that have direct contact with the process.

Thus the determination of the final sensing point location is not part of this standard. However, it should be realised that the sensing point location can have an overall effect on the operation of any fixed gas detection system, irrespective whether the system is safety related or not.

NOTE 1 See IEC 60079-29-2 for guidance on sensor location. For this document, it is assumed that the gas or vapour reaches the sensor.

NOTE 2 See IEC 60079-10-1 for consideration of area classification.

NOTE 3 For example, see ISA-TR84.00.07 for guidance on evaluation of gas system effectiveness.

5.2.3 Sensor filter elements (passive)

Gas sensors may incorporate a passive filter element to protect the sensor gas membrane from airborne dust, dirt or moisture, or may incorporate a metal sintered disk for explosion protection. All types of passive filter elements have a dangerous undetected failure mode (e.g. blockage), therefore require scheduled inspection and proof testing.

The stated safety function per sensing point should consider the intrinsic use of such passive filters, therefore should include within the stated safety function an acceptable response time when a proof test is initiated.

5.2.4 Sensor filter elements (active)

Gas sensors may incorporate an active filter element to condition or change the sensed gas or vapour. These active filters should be specified by the manufacturer and will have a defined life time. All filters of this kind have dangerous undetected failure modes (e.g. blockage, saturation and deactivation) and therefore require scheduled inspection and proof testing.

Gas sensors may incorporate a catalyst filter. Such filters do not have a defined life time, however they will suffer the same effects as passive filters. These filters should be treated as passive filters, unless environmental conditions affect the catalyst material. All filters of this kind have a dangerous undetected failure mode, therefore they require scheduled inspection and proof testing.

5.2.5 Sensor principles

All sensor measuring principles should be evaluated against the suitability of the application. Depending upon the application and principles sensors may become:

– poisoned – unable to detect the target gas;

– inhibited – less sensitive or unable to detect the target gas;
– saturated – unable to perform measurement correctly due to excessive contact with target gas.

NOTE This is typically a temporary effect;

– consumed –less sensitive or unable to detect the target gas because the useful life of the sensor has been consumed;
– de-hydrated – change in sensitivity or accuracy;
– hydrated – change in sensitivity or accuracy;
– subject to the sleep effect – unable to detect low concentration changes;
– subject to optical interference – subject to spurious gas readings;
– subject to optical blockage – unable to detect the target gas.

Some of these sensor conditions can be detected by diagnostics, thus any failure will be ‘dangerous detectable’. Other sensor conditions cannot be detected by diagnostics thus any failure will be ‘dangerous undetectable’ and therefore scheduled inspection and proof testing of the sensor (calibration) is required.

5.2.6 Poisoning and adverse chemical reaction

Particular sensor technologies suffer from common cause failures; airborne substances can inhibit or poison certain sensor technologies (e.g. catalytic sensors) whereas electrochemical sensors can suffer from adverse chemical reactions.

Sensors using such technologies have a dangerous undetected failure mode (application specific) unless sensor diagnostics detect the loss of sensor sensitivity. If poisoning and/or adverse chemical reactions cannot be excluded for an application, scheduled inspection and proof testing of the sensor (calibration) is required.

If these failure modes cannot be excluded for an application, redundant sensors will not improve the safety integrity as these are common cause failures. The safety integrity will be improved in such cases only by using diverse detection principles.

5.2.7 ppm.hr or %vol.hr lifetime

Particular sensor technologies have a ppm.hr or %vol.hr life time. Sensors having lifetime restrictions may have a dangerous undetected failure mode, therefore scheduled inspection and proof testing of the sensor (calibration) is required unless sensor diagnostics detect the incipient end of life.

5.2.8 Negative gas readings

Unlike process measurement, gas sensors have no negative readings of gas values.

NOTE Signals below zero can be caused by zero drift or adverse cross-sensitivities.

5.2.9 Hazard and risk analysis

Gases and vapours generate numerous hazards. They may be flammable, toxic or both. Oxygen levels can be excessive or deficient. Any hazard and risk analysis should consider all hazards associated with gases and vapours, which include short term and long term effects. Gas dispersion should include modelling with consideration to specific gas/vapour densities. The environmental conditions, including the presence of other gases, should be considered.

NOTE See IEC 60079-29-2 for further guidance.

5.2.10 Preventative effectiveness or mitigation effectiveness

Some gas detection functions are preventative, while others only mitigate release consequences. Gas detection functions that mitigate release consequences may not be entirely effective even if they activate. Determining the effectiveness of the mitigation function is outside the scope of this International standard but is more a function of plant specific operation and personnel.

5.2.11 Cross sensitivities

Most gas detection sensors suffer from cross sensitivities which may increase or decrease the response to gas. In general, cross sensitivities can generate spurious alarms or prevent alarms from being tripped. Therefore, particular attention should be paid to the gases or vapours which may occur in an application.

5.2.12 Special states

Gas detection systems use special state signals to indicate the condition of single measuring points, individual control loops or the overall system. Special states may indicate:

– measuring point, control loop or system is in start-up mode;

– measuring point, control loop or system inhibited/override;

– measuring point, control loop or system calibration;

– other system conditions preventing monitoring of gas concentration taking place.

Special states will initiate a contact or other transmittable output signal. The use of these special state signals shall be clearly defined in the stated safety function and it is not always necessary to initiate a ‘safe state’ under a special state condition.

NOTE IEC 60079-29-1 requires special state signals.

5.2.13 Metrological performance standards

Conformance with metrological performance standards is required for all SIL levels.

NOTE International metrological performance standards include IEC 60079-29-1 and IEC 60079-29-4. Other standards can apply in certain jurisdictions including standards for toxic gas and oxygen detection.

The metrological performance standards include electromagnetic compatibility (EMC) testing according to IEC 61326-1. Similar EMC consideration should be given to the associated gas detection equipment.

5.2.14 Fault signal handling

The handling of fault signals shall be clearly defined in the stated safety function. Unlike process shutdown systems it may not be the desired output of a fixed gas detection system to generate a false (spurious trip) shutdown/evacuation process.

5.2.15 Over-range indication

When an application uses catalytic sensor technology it shall generate an unambiguous display (readout) for an over-range measurement.

NOTE This is a requirement of IEC 60079-29-1.

5.2.16 Surrogate calibration

When a target gas is not available for gas sensor calibration it is possible to use a surrogate gas. Surrogate gas calibrations will be less accurate. The use of surrogate gas calibrations should be advised by the manufacturer and should be clearly identified in the associated system safety manual.

Relative sensitivity of the surrogate gas can vary with temperature, humidity, ageing, etc. Also, the times of response and times of recovery of the surrogate gas can differ significantly from those of the target gas. These conditions can affect proof testing.

5.2.17 Maximum/minimum alarm set points

Depending upon the application there may be recommendations not to set alarms above a certain percentage of the measuring range.

To guard against spurious trips due to sensor drift, a minimum alarm set point should be stated.

6 Functional safety management

6.1 Objective

The objective of this clause is to state the minimum functional safety management requirements that any individual, department or organization shall meet with respect to their responsibilities during any phase of a fixed gas detection system life cycle.

6.2 Requirements

A functional safety management system shall be in place during each phase of the fixed gas detection system life cycle. A functional safety management system shall consider the following:

- safety function and safety integrity level;
- uniqueness of the application or design;
- the organizations involved in the total life cycle;
- the scope of supply for each organization.

NOTE Subject to the stated integrity level the rigour of any functional safety management system might change.

Any individual, department or organization who has an involvement in one or more phases of a fixed gas detection system life cycle shall, in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the fixed gas detection system achieves and maintains the required functional safety function and integrity.

Any individual, department or organization which is responsible for carrying out and reviewing each of the safety life-cycle phases shall be identified and be informed, in writing, of the responsibilities assigned to them.

Any individual, department or organization involved in the safety life-cycle activities shall be competent to carry out the activities for which they are accountable. Special attention to the following shall be included:

- knowledge and experience of fixed gas detection systems and relevant local, national and international gas detection standards;
- knowledge and experience of fixed gas detection systems when used as Primary Protection systems;
- knowledge and experience of the use, operation and maintenance of fixed gas detection systems.

Any individual, department or organization which has an involvement in one or more phases of a fixed gas detection system life cycle shall execute safety planning which defines the activities which are required to be carried out to ensure the safety function and safety integrity is achieved or maintained. Safety plans shall be updated as necessary.

Any individual, department or organization who has an involvement with the Hazard and Risk Analysis associated with any fixed gas detection system shall determine both the instantaneous effects of a gas release and any long term and covert effects associated with a gas release.

The manufacturer of the fixed gas detection system, sub-system or a gas detector is responsible for the aspects of placing the fixed gas detection system, sub-system or gas detector on the market. The responsibility shall apply not only to design, construction and production, but also it shall cover the information required for the intended use of the fixed gas detection system, sub-system or gas detector.

Independent review is required for all SIL targets, and the degree of independence shall increase as the SIL target number increases. Table 2 shows the requirements for the rigour of Functional Safety Management pertinent to the SIL target. Where more than one SIL target is defined for different control loops, then the rigour and independence shall comply with the highest SIL target of the entire fixed gas detection system.

Table 2 – Demand for Functional Safety Management (see IEC 61508-1)

	No SIL (0)	SIL 1	SIL 2	SIL 3
Gas detector supplier	A	A	HR	M
Sub-system supplier	A	HR	M	M
Gas Detection System supplier	A	M	M	M
System Integrator or equivalent	A	M	M	M
A = Advisory, HR = Highly recommended, M = Mandatory				

6.3 Competence

Competence is the ability to undertake responsibilities and to perform activities to a recognized standard on a regular basis. Competence is a combination of practical and thinking skills, experience and knowledge. All organizations who have an involvement in one or more phases of a fixed gas detection system life cycle should execute a competency management scheme. Any such competency management scheme should provide evidence that all individuals are competent to carry out the activities for which they are accountable. As a minimum, the following should be addressed when considering the competence of individuals:

– engineering knowledge, training and experience appropriate to the phase which they are accountable for;
– engineering knowledge, training and experience appropriate to the technology (including software) used;
– engineering knowledge, training and experience appropriate to the complexity and novelty of the fixed gas detection system design;
– engineering knowledge, training and experience appropriate to the application or use of the fixed gas detection system;
– knowledge of the legal and safety regulatory requirements;
– adequate management and leadership skills appropriate to their role in the safety life cycle;
– knowledge and training with respect to the appropriate local, national and international standards applicable to fixed gas detection systems, safety instrumented systems and pertinent quality systems, including those standards as specified in Clause 2 of this international standard;
– understanding the potential consequences of a failure;

– training in gas detection and hazardous area emergency response in order to assure that their actions do not reduce the effectiveness of the gas detection system or create further plant safety issues;
– previous experience and its relevance to the specific duties to be performed;
– training or competency in SIL assessment for control systems.

The training, experience and qualifications of all persons involved in any phase of a fixed gas detection system shall be documented.

7 General requirements

7.1 Objective

The objective of Clause 7 is to define the general requirements of a fixed gas detection system.

7.2 Requirements

7.2.1 General

The design of a fixed gas detection system shall be in accordance with the stated Safety Requirements Specification, taking into account all the requirements of this clause.

The use and combination of a gas detector (including the sensor), control unit and a final element shall follow this standard in addition to IEC 61508.

For process industries, IEC 61511 may be used.

A fixed gas detection system shall be designed to ensure easy operation, maintainability and testability.

The action of a fixed gas detection system under special state or gas alarm condition should not automatically switch to a safe state.

7.2.2 Safety and non safety functions

A fixed gas detection system can implement both safety and non-safety functions. The Safety Requirements Specification will clearly define which functions of the fixed gas detection system have an allocated safety integrity level. Where the fixed gas detection system is to implement both safety and non-safety functions then all the hardware and software that can negatively affect any safety function under normal and fault conditions shall comply with the highest safety integrity level.

NOTE It is desirable to have safety functions be separated from non-safety functions whenever possible.

7.2.3 Safety functions of different integrity targets

Where a fixed gas detection system is to implement safety functions of different safety integrity levels then all the hardware and software shall conform to the highest safety integrity level unless it can be shown that the safety function of the lower safety integrity levels cannot negatively affect the safety function of the higher safety integrity levels.

7.2.4 Behaviour under dangerous failure conditions

Requirements:

<u>All SIL-capabilities:</u>

The detection of a dangerous failure (by diagnostics test, proof test or by any other means) in a fixed gas detection system with or without redundancy shall be referenced to the Safety Requirements Specification, and result in initiation of:

a) a specified action to achieve a safe state; or
b) a specified action where the fault is brought to the attention of the operator, who may initiate an action to achieve a safe state; or
c) a specified action where the fault is brought to the attention of the operator, who initiates a repair action so that the safety function is made available within the specified mean time to restoration (MTTR); or
d) a combination of a), b) or c).

The Safety Requirements Specification shall clearly specify the acceptability of spurious trips or system unavailability when a fault is detected.

If the safety function cannot be repaired or restored within the mean time to restoration, then the end user is responsible for initiating additional risk reduction actions. Alternative risk reduction actions should be detailed in the Safety Requirements Specification.

7.2.5 Behaviour under safe failure conditions

Requirements:

All SIL-capabilities:

The detection of a safe failure (by diagnostics test, proof test or by any other means) in a fixed gas detection system with or without redundancy shall be referenced to the Safety Requirements Specification, and result in initiation of:

a) a specified action where the fault is brought to the attention of the operator, who initiates a repair action; or
b) a specified action where the fault is brought to the attention of the operator, who may initiate an action to achieve a safe state; or
c) a specified action to achieve a safe state; or
d) a combination of a), b) or c).

NOTE The response to safe failures might not require immediate action, and the response to safe failures depends strongly on the nature of the failure.

7.2.6 Behaviour under special state conditions

Requirements:

All SIL-capabilities:

Special states other than faults are intentionally initiated. The actions to be taken are specific to the application and shall therefore be specified in the safety manual.

The detection of a special state in a fixed gas detection system with or without redundancy shall be referenced to the Safety Requirements Specification, and result in initiation of;

a) a specified action where the special state is brought to the attention of the operator, who initiates an investigation so that the special state is terminated and the safety function is reset or made available within the specified mean time to restoration (MTTR); or
b) a specified action where the special state is brought to the attention of the operator, who may initiate an action to achieve a safe state; or
c) a specified action to achieve a safe state; or

d) a combination of a), b) or c).

7.2.7 Power supply

7.2.7.1 Characterisation

Power supplies are not included in the characterisation of the safety function when the entire fixed gas detection system is designed to operate in a fail-safe mode for all outputs related to a fault condition.

If fail-safe outputs are not used within the fixed gas detection system then the reliability of the power supply system should be included in the characterisation of the safety function.

7.2.7.2 Requirements

All SIL-capabilities:

a) System with a single power supply: a fault signal shall be initiated if the power supply fails.
b) System with a redundant power supply: no loss of safety function shall occur during transition from one power supply system to the other. An indication should be initiated if either power supply fails. A fault signal should be initiated if both power supplies fail.
c) System supported by an Uninterruptible Power Supply (UPS) system: no loss of safety function shall occur during transition from the power supply system to the UPS. An indication should be initiated if the power supply fails and the fixed gas detection system switches to the UPS. The systems safety function shall describe operational measures which are necessary when the fixed gas detection system is powered from a UPS system which is dependent upon a battery supply (limited duration). A fault signal should be initiated if the UPS system fails.

The fixed gas detection system shall be capable of monitoring d.c. power supply. If the d.c. voltage rises or falls beyond predefined limits a special state shall be signalled.

7.2.8 Gas detector

Requirements:

All SIL-capabilities:

A gas detector, including the sensor is a standard production item as sold by the manufacturer, therefore a gas detector, including the sensor shall conform to IEC 61508-1, IEC 61508-2 and IEC 61508-3.

A gas detector, including the sensor shall conform to the pertinent metrological performance standards (see IEC 60079-29-1 and/or IEC 60079-29-4).

7.2.9 Gas detection control unit (logic solver)

Requirements:

All SIL-capabilities:

A gas detection control unit (logic solver) is a standard production item as sold by the manufacturer, therefore the individual components, including pertinent software shall conform to IEC 61508-1, IEC 61508-2 and IEC 61508-3.

A gas detection control unit (logic solver) shall conform to the pertinent metrological performance standards (see IEC 60079-29-1 and/or IEC 60079-29-4).

7.2.10 Final element (actuator)

Requirements:

<u>All SIL-capabilities</u>:

A final element (actuator) is a standard production item as sold by the manufacturer; therefore, the final element shall conform to IEC 61508-1, IEC 61508-2 and IEC 61508-3.

NOTE If SIL-compliant actuators are not available consideration can be given to the use of actuators which are monitored by external SIL-compliant diagnostic components (e.g. the position monitoring of a ball valve).

7.2.11 Visual indication

7.2.11.1 Characterisation

Visual indication panels are used to display information under normal, alarm state, special state, configuration and maintenance operations of the fixed gas detection system. Visual indication panels can vary in complexity.

Some fixed gas detection systems might not use visual indication panels.

7.2.11.2 Requirements

<u>All SIL-capabilities</u>:

All visual indications shall be unambiguous and may include the following:

– gas values and units of measurement;
– alarm condition;
– under range and over range;
– special state condition;
– configuration data;
– diagnostics data;
– peripheral and/or associated gas detection equipment special state or fault condition.

It shall be possible to set the priority of the above visual indications and those settings shall be documented.

All visualisation panels shall conform to the metrological performance standards.

<u>Additional requirements for SIL-capabilities 2</u>:

A self test facility of all display elements shall be provided on user request. It shall be possible for the user to assess the result of the self test.

7.2.12 Switching outputs

7.2.12.1 Characterisation

Switching outputs provide alarms and special state signals or may initiate safe actions in equipment external to the fixed gas detection system.

7.2.12.2 Requirements

<u>All SIL-capabilities</u>:

Switching outputs shall be triggered by gas alarms and special state conditions, whether they are single, grouped or voted alarms or conditions.

Fault outputs shall be fail-safe.

All switching outputs shall be proof tested regularly. The frequency of the proof test shall be detailed under Maintenance plan.

The configuration of the gas alarm and special state switching outputs are optional; if configured as fail-safe consideration should be given to spurious alarms under a power failure condition.

The function and configuration of all switching outputs shall be specified in the Safety Requirements Specification.

All alarms shall remain tripped until a manual reset has been initiated, unless the Safety Requirements Specification states differently.

All switching outputs shall be capable of operating under their full load conditions as specified by the device manufacturer.

NOTE Commonly these full load conditions will be 60 % of the relay manufacturer's rating to avoid welded contacts.

The safety specification shall specify the maximum number of switching outputs within a complete system, sub-system, voting group, group or individual loops that are off-line (override) for maintenance purposes.

Additional requirements for SIL-capabilities 2:

Either an SIL 2 compliant relay shall be used considering all limitations of use as stated by the relay manufacturer, or two of the three following options shall be applied:

a) Using an output function energised in normal operation mode.
b) Limiting the load of the relay contacts to 60 % of the current rating specified in the component data sheet.
c) Monitoring the input circuit (e.g. relay coil) of the switching outputs.

Additional requirements for SIL-capabilities 3:

Two independent switching outputs each complying with SIL-capability 2 shall be provided for each safety function.

or

An SIL 3 compliant relay shall be used considering all limitations of use as stated by the relay manufacturer.

Monitoring the output circuit (e.g. by using relays with constraint contacts or assessment of a feedback contact) does not improve the relevant safe failure fraction because a possible fault will not be detected until the safety function is actually required. Additional operational procedures is required to initiate the safety function if a fault of this type is detected.

7.2.13 Protocol outputs

7.2.13.1 Characterisation

Safety protocol outputs may be an integral part of the safety function. Non-safety protocol outputs are not part of the safety function and may be used for visualisation, event storage trending, interrogation, and other similar non-safety relevant purposes only.

7.2.13.2 Requirements

Safety protocol outputs shall conform to IEC 61508. Non-safety protocol outputs shall not be capable of adversely affecting the safety function of the fixed gas detection system.

7.2.14 Protocol inputs

7.2.14.1 Characterisation

Safety protocol inputs may be an integral part of the safety function. Non-safety protocol inputs are not part of the safety function and may be used for visualisation, event storage trending, interrogation, and other similar non-safety relevant purposes only.

7.2.14.2 Requirements

Safety protocol inputs shall conform to IEC 61508. Non-safety protocol inputs shall not be capable of adversely affecting the safety function of the fixed gas detection system.

7.2.15 System architecture, PFD and PFH values

The architectural constraints as defined by IEC 61508 apply to a fixed gas detection system. Each gas detector, sub-system and complete system shall conform.

For process industries, IEC 61511 may be used.

The Probability of Failure on Demand (PFD) values as defined by IEC 61508 apply to a fixed gas detection system. The total sum of all sub-system PFD values used in a single gas detection safety loop shall conform to the safety integrity target as stated in the safety specification.

For applications requiring high demand or continuous mode, Probability of Failure on High Demand (PFH) values shall be specified in accordance with IEC 61508.

8 Gas detection unique requirements

8.1 Objectives

The first objective of this clause is to define how to comply with the unique requirements of a fixed gas detection system as a Safety Instrumented System.

The second objective of this clause is to define how associated gas detection equipment which is part of the safety function and contributes to the operation of the fixed gas detection system should conform to this international standard. Associated gas detection equipment includes:

- gas samplers;
- gas multiplexers;
- gas multiplexer control units;
- gas conditioners;

- automatic gas calibration and adjustment units.

If a functional unit is not described in Clause 8, then the procedure in Annex C should be followed to verify the required SIL-capability for this functional unit.

8.2 Requirements

8.2.1 Introduction to gas sampling

In an aspirated system, the pump(s), flow monitoring and final sample conditioning, as well as any features associated with multiplexing, are usually integral with a manufactured system, including sample point conditioning components that may also be included. However, the overall integrity is influenced to a great extent by the selection, installation and maintenance of elements of the gas sampling system, particularly sample tubing as installed and location of sampling point equipment. For requirements and guidance with respect to these aspects reference should be made to IEC 60079-29-2. Design in this area is a highly specialized task and additionally requires compliance with IEC 61508.

8.2.2 Gas sampling

8.2.2.1 Characterisation

Gas aspiration consists of the elements: sample line, gas suction pump, setting of sample flow (bypass or reduction valves), gas aspiration to the sensor and flow monitoring.

8.2.2.2 Requirements

All SIL-capabilities:

The gas aspiration shall be so designed that a loss of continuity or restriction of the gas aspiration shall be detected. Ingress of air or loss of gas to be measured caused by leakage shall be prevented or shall be detected and annunciated.

Inspection of all sample points, sample lines, pumps, filters etc. shall be on a frequent basis. The frequency of inspection is determined by the application, SIL integrity and the environmental conditions.

SIL-capabilities 1 and 2:

The variations of gas flow shall be monitored near the sensor (lower limit or upper limit if necessary). Flow conditions that do not meet the functional requirements, e.g. for response, shall be detected. Two monitoring devices shall be provided as a minimum. These may be flow or pressure/vacuum monitors and shall be critically located. If sample multiplexing (see gas multiplexer) is used, this monitoring location should be between the multiplexing valves and the sensor so as to also detect any failures in the multiplexing module leading to sample delivery errors.

Diagnosis elements shall be implemented with their failure rates to the FMEDA (Failure Mode, Effects and Diagnostic Analysis) but do not have to conform to SIL itself.

Additional requirements for SIL-capability 3:

A protected and tight mounting of the sample lines up to the sensor shall be provided in combination with flow monitoring as specified for SIL capability 1 and 2.

'Protected' means an installation where a leakage caused by mechanical influence will be of low probability, e.g. the sample lines may consist of stainless steel or other material compatible with the sample. Flexible lines should be avoided or protected by being installed in additional tubing or ducting, or in a cabinet closed during normal operation.

'Tight mounting' means the use of welded connections or compression-type tube fittings.

Diagnosis elements shall be implemented with their failure rates to the FMEDA (Failure Mode, Effects and Diagnostic Analysis) but do not have to comply with SIL itself.

8.2.3 Gas multiplexer

8.2.3.1 Characterisation

The gas multiplexer consists of sampling line selection and may include sample line purging or by-passing.

The individual sampling points are selected sequentially. The gas sample from the selected measuring point is passed through the gas multiplexer to be measured at the sensor.

Sample line purging is a process which draws in a fresh gas sample to fill the sample line before the line of this sampling point is selected. This may be done by means of a by-pass pump drawing on the next line to be sampled or drawing on all lines not being sampled at any instant. This decreases the time taken by each individual measurement.

The gas multiplexer presupposes the existence of the gas sampling and gas multiplexer control.

8.2.3.2 Requirements

All SIL-capabilities:

The gas flow shall be monitored for each sampling line near the sensor and near the sampling point (lower limit or upper limit if necessary). Flow conditions that do not meet the functional requirements, e.g. for response time, shall be detected and indicated by a transmittable signal.

The principle of gas sampling shall be applied to protect against ingress of air and blockage. Apart from protection against blockage and leakage diluting samples, precautions shall also be taken to insure that the sample presented to the sensor is not contaminated by the sample from another sample stream.

Additional requirements for SIL-capability 2:

The signals from flow monitoring of all measuring points shall be processed (in module gas multiplexer control) on a continuous basis. A flow shall only be detected at lines actually sampled or purged. The distinction between "flow" and "no flow" by one threshold limit is sufficient.

Additional requirements for SIL-capability 3:

The distinction between "flow" and "no flow" shall be provided by two separate threshold limits (near zero and near set point). Low flow shall be detected in the sample line and leakage flow shall be detected in sample lines not being used.

Inspection of all sample points, sample lines, pumps, filters, valves etc shall be on a frequent basis. The frequency of inspection is determined by the application, SIL-capability and the environmental conditions.

8.2.4 Gas multiplexer control system

8.2.4.1 Characterisation

The gas multiplexer control system selects the measuring point from which gas is passed to the sensor. It ensures that the calculation and assessment of measuring values is associated with the correct measuring point. It also initiates an alarm action to the fixed gas detection system in case of a special state or fault condition occurring within the gas sampler, gas multiplexer or gas multiplexer control system.

In the simplest case the polling of the measuring points may be cyclic. However, it is possible for more complex sequencing be demanded, e.g. event driven sequences.

8.2.4.2 Requirements

All SIL-capabilities:

The gas multiplexer control system shall monitor the correct processing by assessment of status indication within the gas multiplexer control system. If status indication is not correct then a fault shall be indicated.

If the switching is event-driven the prolongation of the maximum cycle time for non activated measuring points shall be within a specified time frame which is application dependent. If it is not in the specified time frame then a fault shall be indicated.

The gas multiplexing control system comprising flow/pressure sensors, logic processing and alarming and transition to a special state logic defines a sub-system safety function that shall itself be demonstrated as attaining the maximum SIL-capability of the safety function where the gas multiplexer module belongs.

8.2.5 Conditioning of measured gas

8.2.5.1 Characterisation

The conditioning of aspirated sample gas may consist of one or more elements including probe, filter, chemical-converter, sample line heater, gas cooler, water trap and de-humidifier.

8.2.5.2 Requirements

Conditioning of measured gas presupposes the existence of the gas sampler and the requirements stipulated in the clause covering gas sampling.

All SIL-capabilities:

Instructions shall be given in the safety manual to allow the user to calculate the allowable operational time of elements with restricted operation time (e.g. where filters are used that can saturate in time). These elements shall be replaced before reaching their operation time. The performance requirements applicable to the conditioning system required for the application shall be specified in the functional unit or gas detection system safety manual for example, the allowable temperature range if a heater or cooler is required.

Additional requirements for SIL-capability 2:

The function of any single element necessary for functional safety shall be either:

- subject to a regime of regular inspections based on the manufacturer's recommendations and a consideration of the site conditions; or
- provided with adequate on-line diagnostics or monitoring to ensure proper operation (e.g. monitoring of the maximum temperature of an electrical gas cooler). Diagnosis elements

shall be implemented with their failure rates to the FMEDA but do not have to comply with SIL itself.

Additional requirements for SIL-capability 3:

Adequate on-line diagnostics or monitoring shall be provided to ensure proper operation (e. g. monitoring of the temperature range of an electrical gas cooler).

Normally SIL 3 will not be achievable by a single chain and typically the whole measuring chain from gas inlet to sensing element will need to be duplicated. Diagnosis elements shall be implemented with their failure rates to the FMEDA but do not have to conform to SIL itself.

8.2.6 Gas sampling by diffusion mode

8.2.6.1 Characterisation

The gas sampling consists of elements such as filters or chemical converters; for example, filters include sintered metal disks, hydrophobic barriers, paper discs etc. Most filters and chemical converters may have restricted operation time due to saturation or degradation.

8.2.6.2 Requirements

All SIL-capabilities:

Instructions shall be given in the safety manual to allow the user to calculate the operation time of elements with restricted operation time (e.g. saturation of filters due to dust). These elements shall be replaced or cleaned before reaching their operation time based on the manufacturer's recommendations and a consideration of the site conditions.

Where there is any type of filter or sintered metal disk comprising a diffusion screen, the installation shall ensure that water or other liquid cannot come into contact and block it, while at the same time permitting free access of gas and vapour. If the manufacturer has a standardised accessory for this, its limitations shall be specified.

Additional requirements for SIL-capability 2:

The function of all components necessary for functional safety shall be inspected frequently or confirmed via on-line diagnostic tests (e.g. automatic calibration).

Additional requirements for SIL-capability 3:

This is not achievable for single functional units unless it can be demonstrated that faults which prevent the sampling gas from reaching the sensor are not credible. In this case there is no additional requirement to SIL-capability 2.

8.2.7 Automatic calibration and adjustment

8.2.7.1 Characterisation

The functional unit automatic calibration consists of the elements; calibration means (e.g. gas cylinder, gas generator, reference gas cell), test gas line, gas suction pump, setting of sample flow (bypass or valves), gas aspiration to sensor (calibration mask or flow cell) and flow monitoring.

The functional unit automatic calibration presupposes the existence of the functional unit automatic calibration control system.

The automatic calibration may or may not include automatic adjustment.

8.2.7.2 Requirements

<u>All SIL-capabilities</u>:

To avoid spurious trips a special state condition shall be activated before automatic calibration is initiated. A plausibility check shall be carried out during application of the test gas, e.g. by defining a tolerance around the existing sensitivity/calibration. The special state condition shall be deactivated immediately after successful calibration. If the calibration fails, the special state shall be deactivated automatically after a defined period, the former calibration data shall be kept and a fault shall be indicated. All these functions shall be implemented in the functional unit 'control of automatic calibration' or the 'fixed gas detection' system.

A calibration is successful if:

– flow rates during calibration are within acceptable limits;
– speed of response when zero or span gas is applied are within a defined set of limits;
– final calibration values are within a specified tolerance or automatic adjustment is made;
– final calibration values after adjustment are within a specified tolerance of the values immediately before adjustment (eg. excessive drift between successive calibrations); and
– final calibration values do not exceed the manufacturer's recommended limits of range of adjustment (eg. cumulatively excessive adjustment).

In addition to the above, precautions against cross-contamination of calibration gases shall be taken in the same basic way as for gas multiplexing.

All automatic calibration events shall be automatically recorded by the functional unit 'control of automatic calibration' or the 'fixed gas detection' system.

Automatic calibration does not replace the need for manual inspection of the fixed gas detection system. Scheduled manual inspection shall be carried out according to the Maintenance plan.

8.2.8 Automatic calibration and adjustment control system

8.2.8.1 Characterisation

The automatic calibration control system selects the sensor for which the calibration procedure is to be executed. It ensures that the special state 'calibration' is entered, monitored and left at the end of the calibration process.

The initiation of the calibration procedure may be performed automatically by a schedule defined in the control unit (e.g. time-driven), by user request or by request from the fixed gas detection system.

8.2.8.2 Requirements

<u>All SIL-capabilities</u>:

The automatic calibration shall only be released for measuring points which are in measuring mode and additionally are not in alarm condition.

In addition to selection of the measuring point the control unit shall monitor the correct processing and assessment of the calibration procedure. It shall ensure that the special state calibration is entered, monitored and left at the end of the process. Existing calibration data (parameters) shall only be replaced after successful calibration.

All calibration results shall be automatically recorded including the interval between calibrations and the time and date of calibration.

Additional operational procedures shall be in place to ensure that the calibration gases used during the automatic calibration process are:

- within their expiry date;
- certified gas mixtures, including the oxygen content where necessary.

NOTE Typically, a 50 % mid-range calibration test gas concentration is applied.

9 Alternative control units (logic solvers)

9.1 Objectives

The objective of Clause 9 is to define how alternative control units (logic solvers) to the manufacturer's dedicated control unit can be used in an overall fixed gas detection system or sub-system.

9.2 Requirements

9.2.1 Performance (metrological)

As a minimum, any alternative control unit (logic solver) shall be demonstrated to conform to metrological performance requirements for fixed gas detection systems and shall be SIL-capable.

9.2.2 Programming of logic

Logic programming of the alternative control unit (logic solver) shall ensure that all special state and fault alarms experienced in fixed gas detection systems are handled in line with this international standard and the pertinent metrological performance standards (see IEC 60079-29-1 and IEC 60079-29-4).

NOTE For guidance on logic solver programming, see IEC 61511.

Special attention shall be given to the competency of individuals when alternative logic solvers are used in a fixed gas detection system application (See Clause 7).

10 Factory acceptance testing

10.1 Objectives

The objective of this clause is to outline the minimum requirements, including the necessary documentation which should be executed during the phase of Factory Acceptance Testing.

10.2 Requirements

10.2.1 Planning

The need for a Factory Acceptance Test should be specified during the design and engineering phase or in the scope of supply and should include as a minimum:

– the types of tests to be performed;
– the PASS/FAIL criteria, including when to abort the tests subject to a single or multiple test failures;
– procedures for the recording of test data/results and the hardware/software versions of the equipment under test;

- procedures for corrective actions;
- procedures for system modifications or changes;
- procedures for conflict management;
- minimum system configuration requirements;
- dependencies on third party equipment or interfaces;
- test equipment to be used, supported by valid equipment calibration certificates;
- test gases to be used, supported by valid gas composition certificates;
- test persons' competencies and persons in attendance;
- the location of the protected area and any special flammable or toxic gas precautions;
- a description of any ‘black box’ testing; and
- exclusions.

NOTE Factory acceptance testing normally applies to sub-systems and systems, but not standalone gas detectors unless separately stated in the equipment supply contract.

Where the total system is the responsibility of a system integrator, then the planning of the Factory Acceptance Test is the responsibility of the system integrator unless stated otherwise.

10.2.2 Execution

The Factory Acceptance Test should be conducted in accordance with the Factory Acceptance Test plan.

Before the Factory Acceptance Test is performed all documentation shall be checked for:

- completeness;
- correct revision;
- whether all documents are approved for system construction (AFC) as a minimum.

If there is a failure during the Factory Acceptance Test, the reason for the failure should be identified and documented. A decision should be taken whether to:

- repair the failure and re-test;
- ignore the failure and complete the system test;
- abort the complete test program if the failure affects the total system,, thus allowing the failure to be repaired, with a new test date being arranged; or
- partially complete the tests and plan an additional partial Factory Acceptance Test.

If during the Factory Acceptance Test any modifications or changes to the system are performed then these changes should be subject to a safety analysis to determine:

- the extent of the impact on each safety function; and
- the extent of any re-test which should be defined and implemented.

11 Installation and commissioning

11.1 Objectives

The objective of this clause is to outline the minimum requirements, including the necessary documentation which should be executed during the phase of Installation and Commissioning.

11.2 Requirements

11.2.1 Planning

Installation methods and commissioning procedures should be specified during the design phase of the fixed gas detection system and should include as a minimum:

- the installation activities;
- any special precautions required during installation (as recommended by the device suppliers);
- the person, department or organization responsible for the installation activities;
- precautions to take when the installation is within an hazardous area;
- electrical tests required to satisfy the electrical installation is correct (before the system is energised);
- the types of tests to be performed on system start-up;
- the PASS/FAIL criteria, including when to abort the tests subject to a single or multiple test failures;
- procedures for the recording of test data/results and the hardware/software versions of the equipment under test;
- procedures for corrective actions;
- procedures for system modifications or changes;
- procedures for conflict management;
- test equipment to be used, supported by valid equipment calibration certificates;
- test gases to be used, supported by valid gas composition certificates;
- test persons' competencies and persons in attendance;
- any special fFlammable or toxic gas precautions; and
- exclusions.

11.2.2 Execution

The installation should be conducted in accordance with the installation plan.

The commissioning should be conducted in accordance with the commissioning plan.

Before installation and commissioning, all documentation shall be checked for:

- completeness;
- correct revision;
- approval for system installation and commissioning.

If there is a failure during commissioning, the reason for the failure should be identified and documented. A decision should be taken whether to:

- repair the failure and continue with the commissioning exercise;
- ignore the failure and complete the commissioning exercise;
- abort the complete commissioning exercise if the failure affects the total system, thus allowing the failure to be repaired, with a new commissioning date being arranged; or
- partially complete the commissioning exercise and plan an additional final commissioning activity.

If during the commissioning exercise any modifications or changes to the system are performed then these changes should be subject to a safety analysis to determine:

- the extent of the impact on each safety function; and

– the extent of any re-test which should be defined and implemented.

All modifications shall be documented.

12 System validation[1]

12.1 Objectives

The objective of this clause is to outline the minimum requirements, including the necessary documentation which should be executed during the phase of system Validation.

NOTE The system validation considers the overall system and the correct integration of components of different manufacturers.

12.2 Requirements

12.2.1 Planning

The need for a System Validation Test should be specified during the design phase of the fixed gas detection system and should include as a minimum:

– validation methods to ensure that the installed fixed gas detection system performs the safety function as stated in the Safety Requirements Specification;
– validation methods to ensure that the installed fixed gas detection system operates correctly under:
  • normal operation;
  • abnormal (misuse) operation;
  • special state condition; and
  • fault condition.
– a method to include any system modification which may have been implemented during the Factory Acceptance Test, system Installation or system commissioning;
– validation of persons' competencies and persons in attendance; and
– procedures for the recording of test data/results and the hardware/software versions of the equipment under test.

12.2.2 Execution

The System Validation Test should be conducted in accordance with the System Validation Test plan.

Before the System Validation Test is performed all documentation shall be checked:

– for completeness;
– for correct revision; and
– to see whether all documents are approved for system construction and installation (AFCI) as a minimum.

If there is a failure during the System Validation Test, the reason for the failure shall be identified and documented. A decision shall be taken whether to:

– repair the failure and re-validate;
– ignore the failure and complete the system validation;

1 Commonly known as Site Acceptance Test (SAT).

– abort the complete validation program if the failure affects the total system,, thus allowing the failure to be repaired, with a new validation date being arranged; or
– partially complete the validation and plan an additional partial System Validation Test.

If during the System Validation Test any modifications or changes to the system are performed then these changes should be subject to a safety analysis to determine:

– the extent of impact on each safety function; and
– the extent of re-test which should be defined and implemented.

Until all of the requirements as detailed in the System Validation Test are validated with respect to the Safety Requirements Specification, the fixed gas detection system cannot be considered as operational.

13 Operation and maintenance

13.1 Objectives

The objective of this clause is to outline the minimum requirements, including the necessary routine service requirements, including proof testing which should be executed during the phase of operation and maintenance.

13.2 Requirements

13.2.1 Planning

The need for operation and maintenance planning should be specified during the design phase of the fixed gas detection system and should include as a minimum:

– detailed records of the system's performance during normal operation, including special state and fault conditions;
– the number of demands placed on the system;
– any misuse or abnormal operation of the system;
– applicable environmental data associated with each measuring point;
– the frequency of scheduled system maintenance activities;
– the maximum number of safety loops which are in override during any maintenance activities;
– additional operational measures to be taken during any maintenance activities;
– detailed maintenance records including faults found, corrective or repair actions taken, spare parts used, consumables used and any changes of system performance which may, in the future, affect the safety function;
– detailed proof test results; and
– detailed corrective actions taken if a proof test fails.

13.2.2 Execution

The fixed gas detection system shall be operated as detailed in the overall system safety manual and any pertinent individual equipment operating manuals.

Individuals operating, responding to or maintaining the fixed gas detection system shall be competent and authorised to do so.

NOTE 1 See 6.3 for competency.

The fixed gas detection system shall be maintained as detailed in the overall system maintenance plan. Only spare parts and consumables listed in the safety manual or individual equipment maintenance manuals shall be used.

The fixed gas detection system shall be proof tested as detailed in the system safety manual.

The effectiveness of the proof test will be dependent upon how close to the "as new" condition the system is restored. For the proof test to be fully effective, it will be necessary to detect 100 % of all dangerous failures. Although in practice 100 % is not easily achieved for other than low-complexity E/E/PE safety-related systems, this should be the target. As a minimum, all the safety functions which are executed are checked according to the E/E/PES Safety Requirements Specification. If separate channels are used, these tests are done for each channel separately.

All activities shall be clearly documented.

14 System modification

14.1 Objectives

The objective of this clause is to outline the minimum requirements, including the necessary documentation which should be executed during the phase of system modification.

14.2 Requirements

14.2.1 Planning

Modifications to any fixed gas detection system shall be planned, reviewed and authorized prior to any modification being performed. The plan shall demonstrate an acceptable level of safety during and after the modification.

Planning shall include:

– impact analysis;
– continuation of the fixed gas detection safety function and safety integrity during the modification process;
– alternative measures required to ensure that the safety integrity level is maintained;
– associated hazardous area demands (Explosion Protection Documentation);
– validation methods to ensure that the modification has been performed correctly and all associated functions (not modified) have not been affected;
– emergency plans if the modification is not performed on time or the modification cannot be completed, or an unavoidable event occurs;
– detailed descriptions of the competencies of individuals who will perform the modification;
– the documentation control process; and
– training of personnel after the modification is complete, including service routines, spare parts inventory and operational procedures.

14.2.2 Execution

A modification activity shall not commence without proper authorisation.

All modifications shall be documented, verified and validated, and follow the modification plan, modification documents and modification instructions.

Any deviation from the modification plan shall be authorised and if necessary, a new impact analysis should be performed. If the impact analysis reveals unacceptable risks then the modification should cease and the emergency plan is to be followed.

Upon completion of the modification the entire part system or complete system shall be validated to prove the safety function.

15 System decommissioning

15.1 Objectives

The objective of this clause is to outline the minimum requirements, including the necessary documentation which should be executed during the phase of system decommissioning.

15.2 Requirements

15.2.1 Planning

The decommissioning or part decommissioning of any fixed gas detection system shall be planned, reviewed and authorized prior to the decommissioning being performed. The plan shall demonstrate an acceptable level of safety during and after partial or full decommissioning.

Planning shall include:

- an impact analysis;
- if necessary, how to ensure the continuation of the fixed gas detection system's safety function(s) and safety integrity during the decommissioning process;
- alternative measures required to ensure that the safety integrity level is maintained during the decommissioning process;
- associated hazardous area demands;
- validation of the remaining system if part of the original system is to be decommissioned;
- emergency plans if the decommissioning is not performed on time or the decommissioning cannot be completed, or an unavoidable event occurs;
- detailed descriptions of the competencies of individuals who will perform the decommissioning;
- the documentation control process; and
- training of personnel after the decommissioning is complete, including any changes in operational procedures.

15.2.2 Execution

A decommissioning activity shall not commence without proper authorisation.

All stages of the decommissioning plan shall be documented as they occur, verified and validated, and follow the decommissioning plan.

Any deviation from the decommissioning plan shall be authorised and if necessary, a new impact analysis should be performed. If the impact analysis reveals unacceptable risks then the decommissioning should cease and the emergency plan shall be followed.

Upon completion of the decommissioning activity the entire part system or complete system which has been decommissioned shall be disposed of correctly.

Following the decommissioning activity all relevant staff should be re-trained.

16 Documentation

16.1 Objectives

The objective of this clause is to outline the minimum requirements for all supporting documentation necessary irrespective of the life cycle phase.

16.2 Requirements

All single documents, including individual instrument operating manuals, safety manuals, electrical schematics, parts lists, data sheets etc., should be:

– fit for purpose and applicable to the application;
– accurate and easy to understand; and
– revision controlled.

NOTE The documents are often to be supplied to system integrators.

All document dossiers supplied to support a complete fixed gas detection system should also:

– be indexed and revision controlled;
– be structured to make information easily available;
– include pertinent information for each part of the life cycle;
– contain all results from Factory Acceptance Tests (FAT), Commissioning and Site Validation (SAT);
– include recommended maintenance activities, complete with a supporting test program and record sheets;
– include recommended proof test activities, complete with a supporting test program and record sheets; and
– list recommended operational spare parts.

A total Safety Manual should be compiled which includes as a minimum the following:

– safety function and integrity per safety loop;
– restrictions of use, including consumable parts e.g. filters;
– operational procedures;
– maintenance procedures;
– a fault finding guide; and
– override procedures.

All product certificates should be supplied with the associated test report where available.

Revision control of all documents should clearly state the product or system to which it applies, including the hardware revision and software version of the product or system.

Annex A
(informative)

Typical Applications

A.1 Typical diffusion applications

A.1.1 Application 1

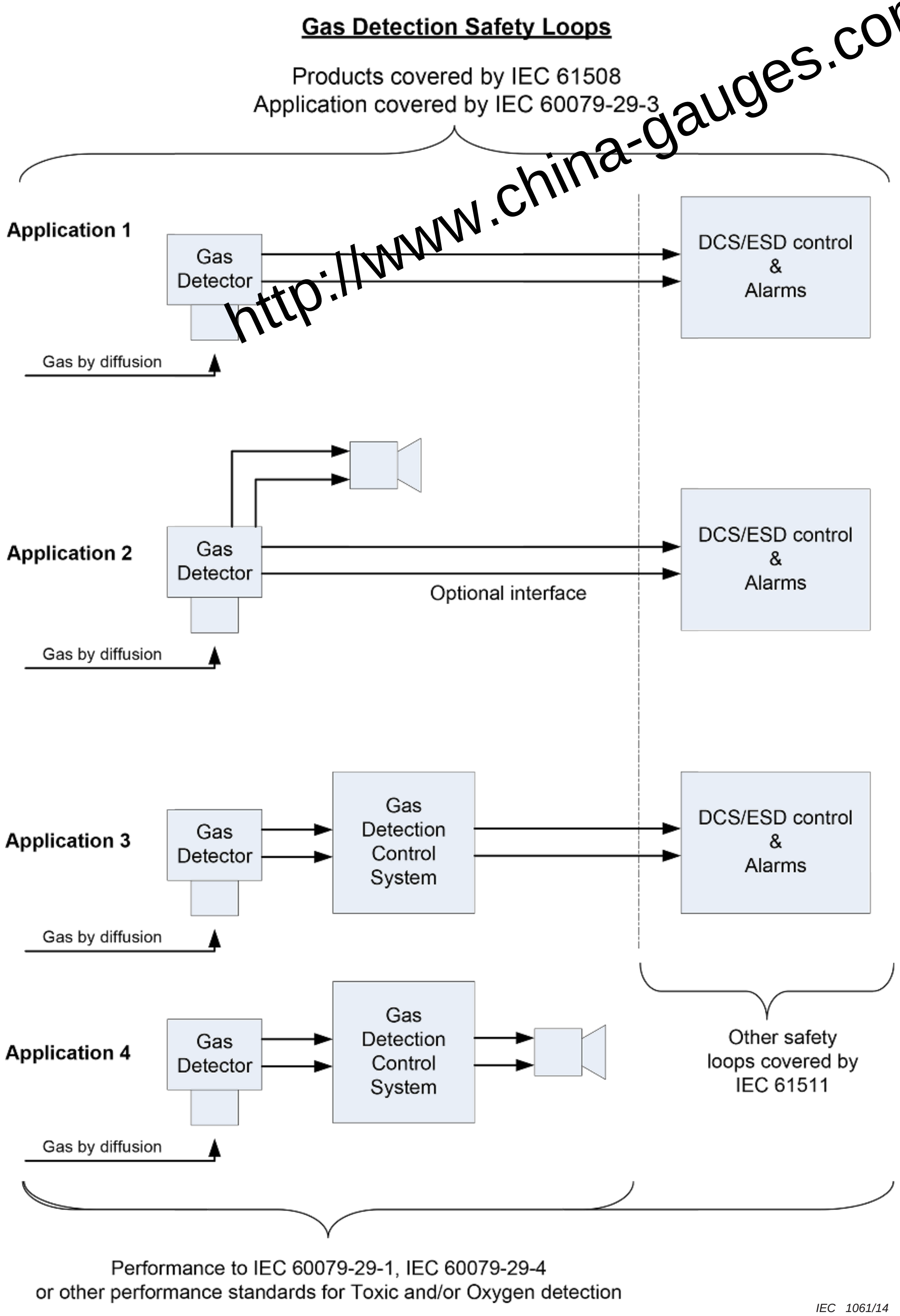


Figure A.1 – Gas detection safety loops

This application covers the use only of a fixed gas detector which is typically integrated into a DCS (Distributed Control System) or ESD (Emergency Shut-down) control system (see Figure A.1). The DCS or ESD control system performs the system logic and initiates the safety action.

The gas detector for this application is designed and manufactured in accordance with the IEC 61508 series. The supply, application, integration and operation for this application are covered by this standard.

A.1.2 Application 2

This application covers the use only of a fixed gas detector which performs the system logic and initiates the safety action (see Figure A.1).

The gas detector for this application is designed and manufactured in accordance with the IEC 61508 series. The supply, application, integration and operation for this application are covered by this standard.

A.1.3 Application 3

This application covers the use of a fixed gas detection system which acts as a sub-system of a larger integrated system (see Figure A.1). This sub-system is then integrated in to a DCS or ESD control system. The DCS or ESD control system performs the final system logic and initiates the safety action.

The fixed gas detection sub-system for this application is designed and manufactured under the IEC 61508 series. The supply, application, integration and operation for this application are covered by this standard.

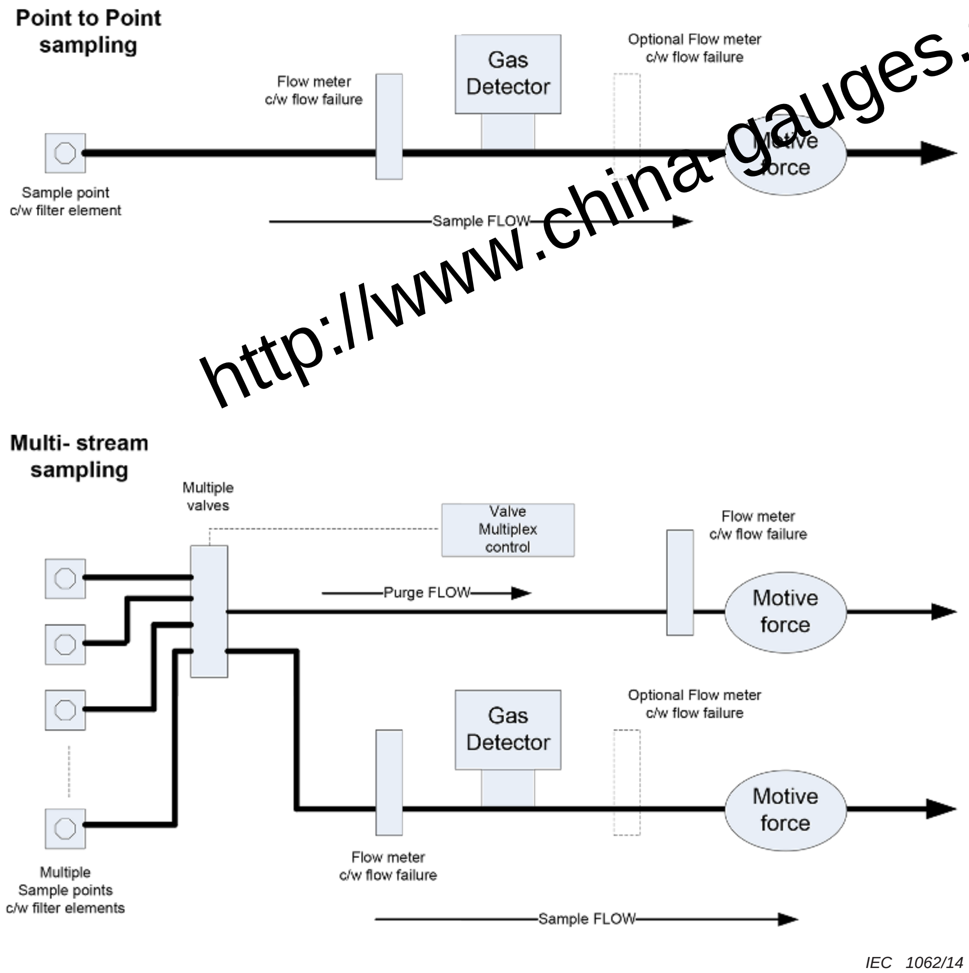
A.1.4 Application 4

This application covers the use of a complete fixed gas detection system which acts as the total safety system (see Figure A.1).

The fixed gas detection system for this application is designed and manufactured under the IEC 61508 series. The supply, application, integration and operation for this application are covered by this standard.

A.2 Typical sampling applications

A.2.1 Point to Point sampling



It is necessary that the valve multiplexer control system shall be part of the gas detection control system or be integrated into the gas detection control system to ensure that any gas alarm event is contributed to the correct sample point (location).

Figure A.2 – Typical gas detector aspiration configurations

A point to point sampling system encompasses three main hardware items other than the gas detector (see Figure A.2). These three items are:

a) a sample point which normally includes a particle filter or equivalent;

b) flow indication complete with a single or dual failure (low and/or high) signal; and

c) a ‘motive force’.

NOTE A motive force could be an electromechanical pump, air eductor or some other means to draw a sample gas.

All three hardware items are connected together using a sample line. The sample line material should be chosen carefully as some materials may be affected by the target gas or interfere with the target gas. The point to point sampling system may include a sample conditioning system (not illustrated).

The flow meter labelled “optional” positioned after the gas detector in Figure A.2 can be an alternative to the other flow meter or can be implemented in addition to the other one.

A.2.2 Multi-stream sampling

A multi-stream sampling system encompasses four main hardware items other than the gas detector (see Figure A.2). These four items are:

a) sample points which normally include a particle filter or equivalent;

b) a multiple valve assembly and a valve multiplex controller;

c) flow indication complete with a single or dual failure (low and/or high) signal for the sample line and flow indication complete with a single or dual failure (low and/or high) signal for the purge line; and

d) a 'motive force'.

NOTE A motive force could be an electromechanical pump, air eductor or some other means to draw a sample gas, with a separate motive force for the purging of sample lines.

All four hardware items are connected together using sample and purge lines. The sample line material should be chosen carefully as some materials may be affected by the target gas or interfere with the target gas. The multi-point sampling system may include a sample conditioning system (not illustrated). The valve multiplex control system should be linked with the gas detection system to ensure that the gas sample being analysed matches with the sensing point location within the logic of the gas detection control unit.

The flow meter labelled "optional" positioned after the gas detector in Figure A.2 can be an alternative to the other flow meter or can be implemented in addition to the other one.

Annex B
(informative)

Cross references between standards

IEC 60079-29-3		IEC 61508	IEC 61511
Clause 1	Scope	Clause 1	Clause 1
Clause 2	Normative references	Clause 2	Clause 2
Clause 3	Definitions	Clause 3	Clause 3
Clause 4	Conformance to this standard	Clause 4	Clause 4
Clause 5	Gas Detection unique deviations		
Clause 6	Functional Safety Management	Clause 6	Clause 5
Clause 7	General requirements	Clause 7.10	Clause 11
Clause 8	Gas Detection unique requirements	Clause 7.10	Clause 11
Clause 9	Alternative logic solvers	Clause 7.10	Clause 12
Clause 10	Factory acceptance testing	Clause 7.18	Clause 13
Clause 11	Installation & Commissioning	Clause 7.9 & 7.13	Clause 14
Clause 12	Validation (SAT)	Clause 7.8 & 7.14	Clause 15
Clause 13	Operation & Maintenance	Clause 7.7 & 7.15	Clause 16
Clause 14	System modification	Clause 7.16	Clause 17
Clause 15	System decommissioning	Clause 7.17	Clause 18
Clause 16	Documentation	Clause 5	Clause 19

IEC 1063/14

NOTE The clauses mentioned in Figure B.1 relate to the editions of IEC 61508:2010 and IEC 61511:2003.

Figure B.1 – Cross references between standards

Annex C
(informative)

Transformation of requirements

C.1 General

This annex tries to relate the demands of the generic standard (IEC 61508 series), other applications standards (IEC 61511 series) and other safety standards to the requirements of a fixed gas detection system, thus this international standard.

“Characteristic” shows the basic philosophy on functional safety. “Transformation” shows the specific interpretation for fixed gas detection systems.

For equipment not covered by this international standard the philosophy of this annex should be followed to define specific requirements.

Additionally, the tables in IEC 61508-2 and IEC 61508-3 and this annex should be used to determine the SIL-capability of such equipment.

C.2 SIL capability 1

C.2.1 Characteristic

Equipment used for a safety function should be designed, manufactured and implemented under an appropriate safety management system that includes requirements for verification, functional safety assessment and competency. Calculation of the safe failure fraction is only required (as specified in IEC 61508-2) for complex modules.

Avoidance of faults is achieved by selection of components, e.g. application of well-proven components. The safety relevant parts of the system are checked at regular intervals. The occurrence of a fault may lead to the loss of the safety function.

C.2.2 Transformation

The system should have demonstrated conformance with IEC 60079-29-1, IEC 60079-29-4 or other metrological standards and should be maintained in respect to the manufacturer's instructions. Additionally to the metrological standards, requirements for the functional safety of alarm outputs, power supply and special state conditions are stated. A plausibility check of the user input should be carried out, e.g. the setting of alarm levels should only be possible within the measuring range.

All equipment should be arranged such that on loss of power, a special state or fault condition is realised and a known state is initiated. Initiation to the safe state may be automatic or manual in response to any type of alarm condition.

For equipment that depends on software to achieve the safety function requirements, the software should meet the requirements of IEC 61508-3 for SIL 1.

C.3 SIL capability 2

C.3.1 Characteristic

For simple equipment the safe failure fraction is assumed to be between 60 % and 90 % if the hardware fault tolerance is 0 (IEC 61508-2). For complex equipment the safe failure fraction should be between 60 % and 90 % if the hardware fault tolerance is 1 or should be between 90 % and 99 % if the hardware fault tolerance is 0 (IEC 61508-2).

The equipment will include the means to check, at regular intervals, any functions necessary to achieve the safety functions required by the gas detection system.

C.3.2 Transformation

Additionally to SIL-capability 1 self testing facilities for hardware and software should be available during each start up period and on user request. The maintenance plan should include the check of all safety related parts. Depending on the application additional operational procedures are required, e.g. shortened calibration intervals or the replacement of filters should be considered under harsh environmental conditions. Special states which are automatically activated in normal operation of the fixed gas detection system should be indicated and alarmed. It should be possible to check the parameter settings during operational mode.

For equipment that depends on software to achieve the safety function requirements, the software should meet the requirements of IEC 61508-3 for SIL 2.

C.4 SIL capability 3

C.4.1 Characteristic

For simple equipment the safe failure fraction is assumed to be between 60 % and 90 % if the hardware fault tolerance is 1 or should be between 90 % and 99 % if the hardware fault tolerance is 0 (IEC 61508-2). For complex equipment the safe failure fraction should be between 90 % and 99 % if the hardware fault tolerance is 1 or should be ≥ 99 % if the hardware fault tolerance is 0 (IEC 61508-2).

The occurrence of a single fault should not lead to the loss of the safety function. The accumulation of undetected faults may lead to the loss of the safety function because not all possible faults will be detected.

C.4.2 Transformation

Additionally to SIL-capability 2 the safety related parts of the gas detection system including output signals should be designed such that a single failure should not lead to a loss of the safety function. Whenever reasonable practicable a single failure should be detected.

For equipment that depends on software to achieve the safety function requirements, the software should meet the requirements of IEC 61508-3 for SIL 3.

Bibliography

IEC 60079-10-1, *Explosive atmospheres – Part 10-1: Classification of areas – Explosive gas atmospheres*

IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 61511-2, *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1*

IEC 61511-3, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

ISA-TR84.00.07, *Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™