

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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2014 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

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

About the IEC

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

About IEC publications

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

IEC Catalogue - webstore.iec.ch/catalogue

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

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

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

A propos de l'IEC

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

A propos des publications IEC

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

Catalogue IEC - webstore.iec.ch/catalogue

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

Recherche de publications IEC - www.iec.ch/searchpub

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

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

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



IEC 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



ICS 29.260.20

ISBN 978-2-8322-1496-1

Warning! Make sure that you obtained this publication from an authorized distributor.

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope	10
2 Normative references	11
3 Terms and definitions	11
4 Requirements	13
4.1 General.....	13
4.2 Demand rate	13
5 Gas detection unique features	13
5.1 Objective	13
5.2 Features	14
5.2.1 General	14
5.2.2 Sensor location.....	14
5.2.3 Sensor filter elements (passive).....	14
5.2.4 Sensor filter elements (active)	14
5.2.5 Sensor principles	14
5.2.6 Poisoning and adverse chemical reaction	15
5.2.7 ppm.hr or %vol.hr lifetime	15
5.2.8 Negative gas readings	15
5.2.9 Hazard and risk analysis.....	15
5.2.10 Preventative effectiveness or mitigation effectiveness	16
5.2.11 Cross sensitivities.....	16
5.2.12 Special states	16
5.2.13 Metrological performance standards	16
5.2.14 Fault signal handling.....	16
5.2.15 Over-range indication	16
5.2.16 Surrogate calibration	16
5.2.17 Maximum/minimum alarm set points	17
6 Functional safety management	17
6.1 Objective	17
6.2 Requirements	17
6.3 Competence	18
7 General requirements	19
7.1 Objective	19
7.2 Requirements	19
7.2.1 General	19
7.2.2 Safety and non safety functions	19
7.2.3 Safety functions of different integrity targets	19
7.2.4 Behaviour under dangerous failure conditions.....	19
7.2.5 Behaviour under safe failure conditions	20
7.2.6 Behaviour under special state conditions	20
7.2.7 Power supply	21
7.2.8 Gas detector	21
7.2.9 Gas detection control unit (logic solver)	21
7.2.10 Final element (actuator).....	22
7.2.11 Visual indication	22

7.2.12	Switching outputs	22
7.2.13	Protocol outputs	24
7.2.14	Protocol inputs	24
7.2.15	System architecture, PFD and PFH values	24
8	Gas detection unique requirements	24
8.1	Objectives	24
8.2	Requirements	25
8.2.1	Introduction to gas sampling	25
8.2.2	Gas sampling	25
8.2.3	Gas multiplexer	26
8.2.4	Gas multiplexer control system	27
8.2.5	Conditioning of measured gas	27
8.2.6	Gas sampling by diffusion mode	28
8.2.7	Automatic calibration and adjustment	28
8.2.8	Automatic calibration and adjustment control system	29
9	Alternative control units (logic solvers)	30
9.1	Objectives	30
9.2	Requirements	30
9.2.1	Performance (metrological)	30
9.2.2	Programming of logic	30
10	Factory acceptance testing	30
10.1	Objectives	30
10.2	Requirements	30
10.2.1	Planning	30
10.2.2	Execution	31
11	Installation and commissioning	31
11.1	Objectives	31
11.2	Requirements	32
11.2.1	Planning	32
11.2.2	Execution	32
12	System validation	33
12.1	Objectives	33
12.2	Requirements	33
12.2.1	Planning	33
12.2.2	Execution	33
13	Operation and maintenance	34
13.1	Objectives	34
13.2	Requirements	34
13.2.1	Planning	34
13.2.2	Execution	34
14	System modification	35
14.1	Objectives	35
14.2	Requirements	35
14.2.1	Planning	35
14.2.2	Execution	35
15	System decommissioning	36
15.1	Objectives	36
15.2	Requirements	36

15.2.1	Planning	36
15.2.2	Execution	36
16	Documentation	37
16.1	Objectives.....	37
16.2	Requirements	37
Annex A (informative)	Typical Applications	38
A.1	Typical diffusion applications	39
A.1.1	Application 1.....	39
A.1.2	Application 2.....	40
A.1.3	Application 3.....	40
A.1.4	Application 4.....	40
A.2	Typical sampling applications.....	41
A.2.1	Point to Point sampling	41
A.2.2	Multi-stream sampling.....	42
Annex B (informative)	Cross references between standards.....	43
Annex C (informative)	Transformation of requirements.....	44
C.1	General.....	44
C.2	SIL capability 1	44
C.2.1	Characteristic	44
C.2.2	Transformation	44
C.3	SIL capability 2	44
C.3.1	Characteristic	44
C.3.2	Transformation	45
C.4	SIL capability 3	45
C.4.1	Characteristic	45
C.4.2	Transformation	45
Bibliography.....		46
Figure 1 – Gas Detection System Architecture		8
Figure 2 – Related Safety Instrumented System Standards.....		10
Figure A.1 – Gas detection safety loops.....		39
Figure A.2 – Typical gas detector aspiration configurations.....		41
Figure B.1 – Cross references between standards		43
Table 1 – Typical Job Descriptions and Most Relevant Clauses		9
Table 2 – Demand for Functional Safety Management (see IEC 61508-1)		18

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").

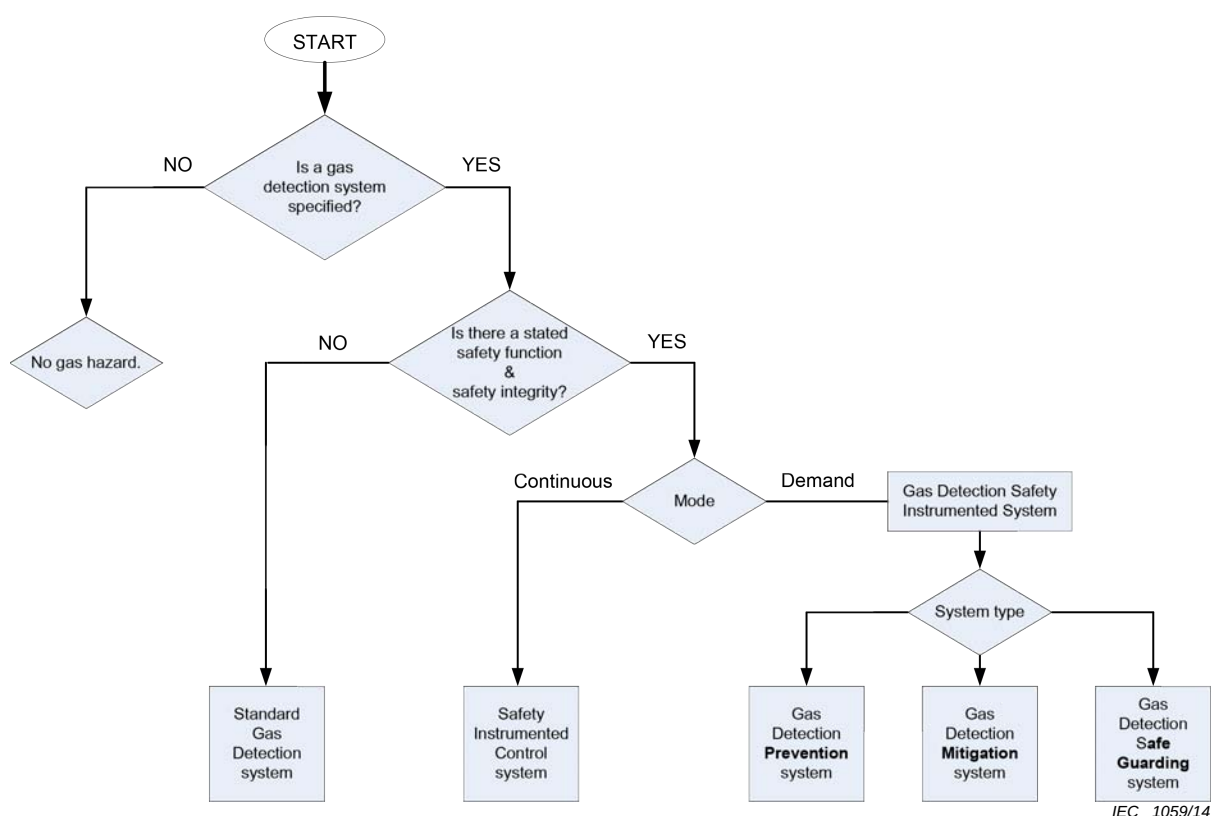


Figure 1 – Gas Detection System Architecture

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.

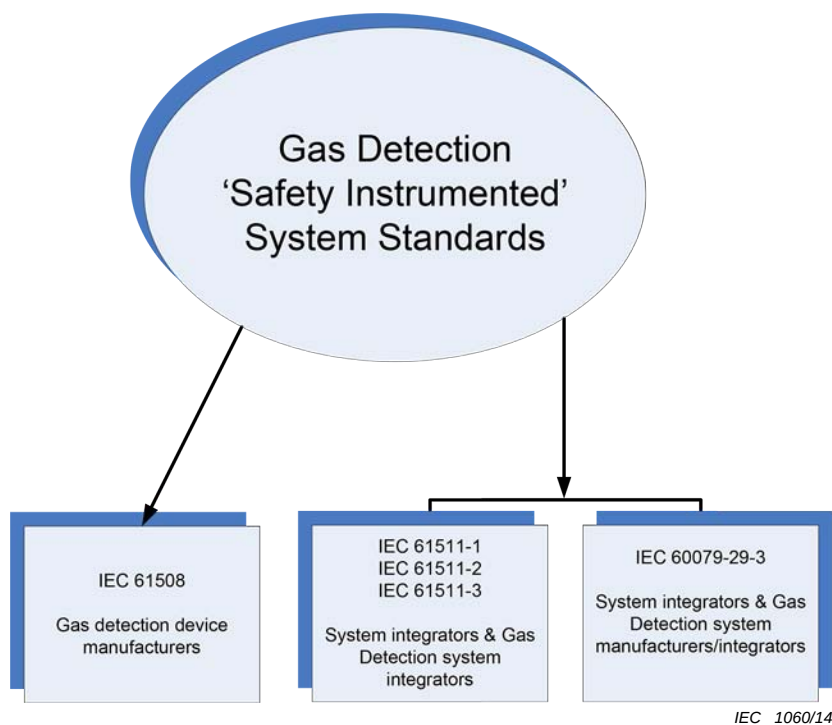


Figure 2 – Related Safety Instrumented System Standards

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:

All SIL-capabilities:

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:

All SIL-capabilities:

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

All SIL-capabilities:

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.

Additional requirements for SIL-capabilities 2:

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

All SIL-capabilities:

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

All SIL-capabilities:

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

All SIL-capabilities:

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 flammable 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 validation¹

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

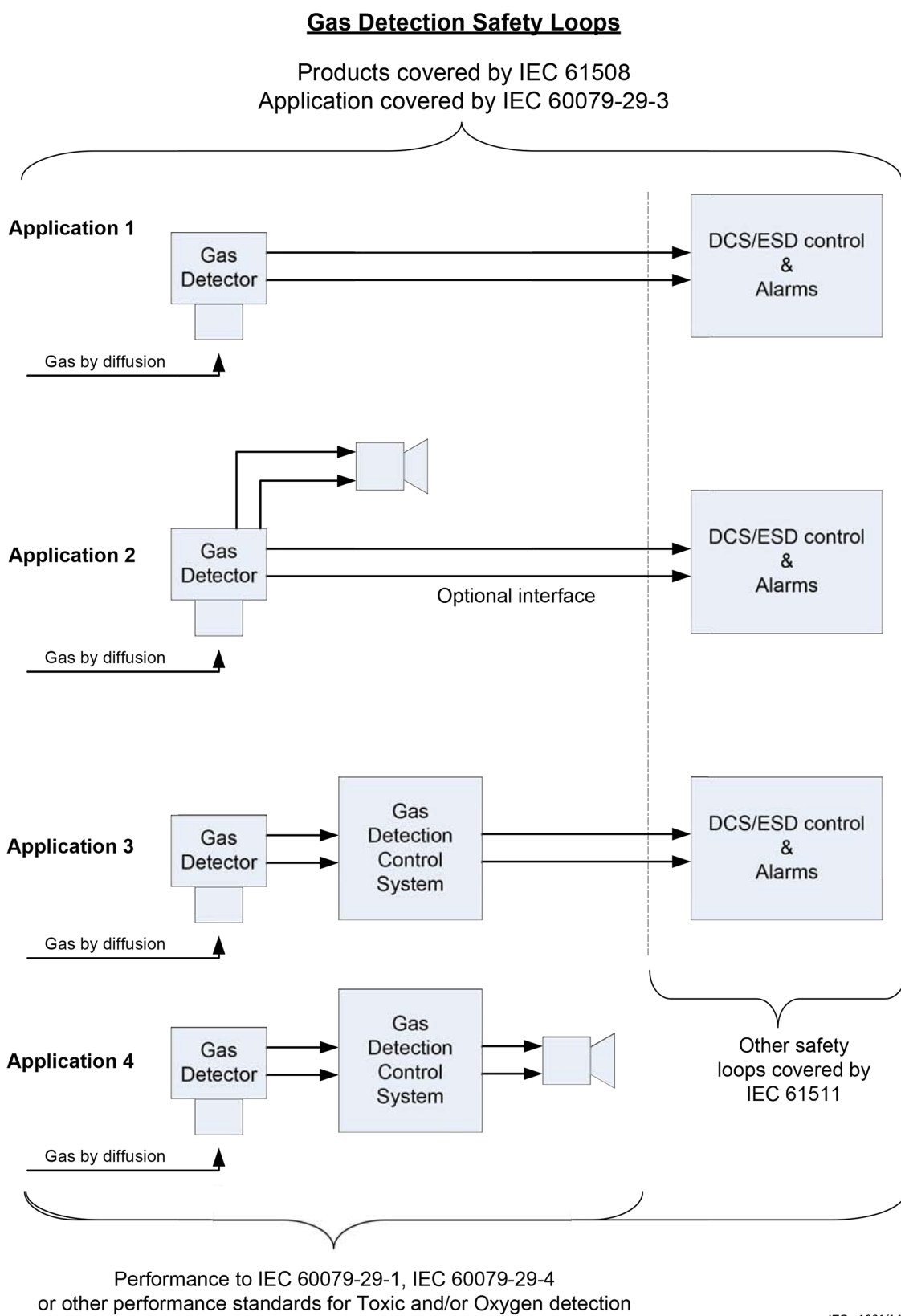


Figure A.1 – Gas detection safety loops

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.

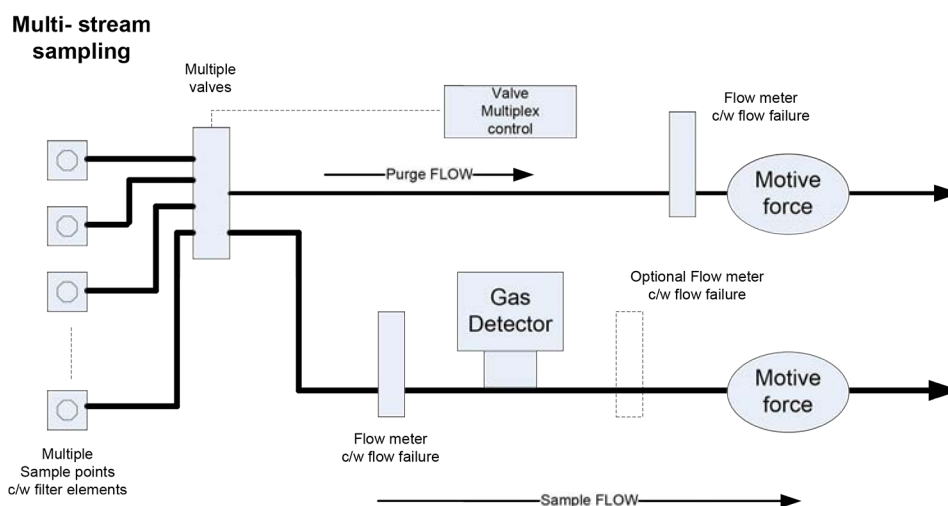
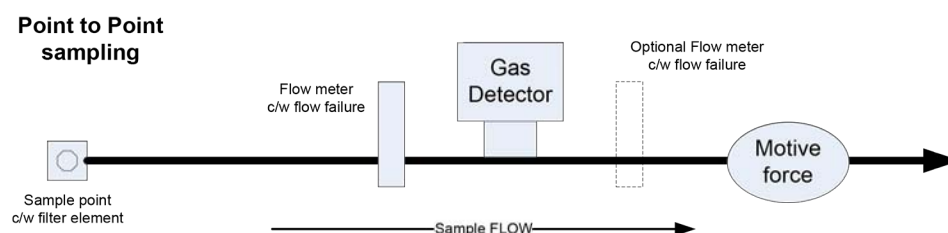
A.1.4 Application 4

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



IEC 1062/14

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 sample point which normally includes a particle filter or equivalent;
- flow indication complete with a single or dual failure (low and/or high) signal; and
- 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'.

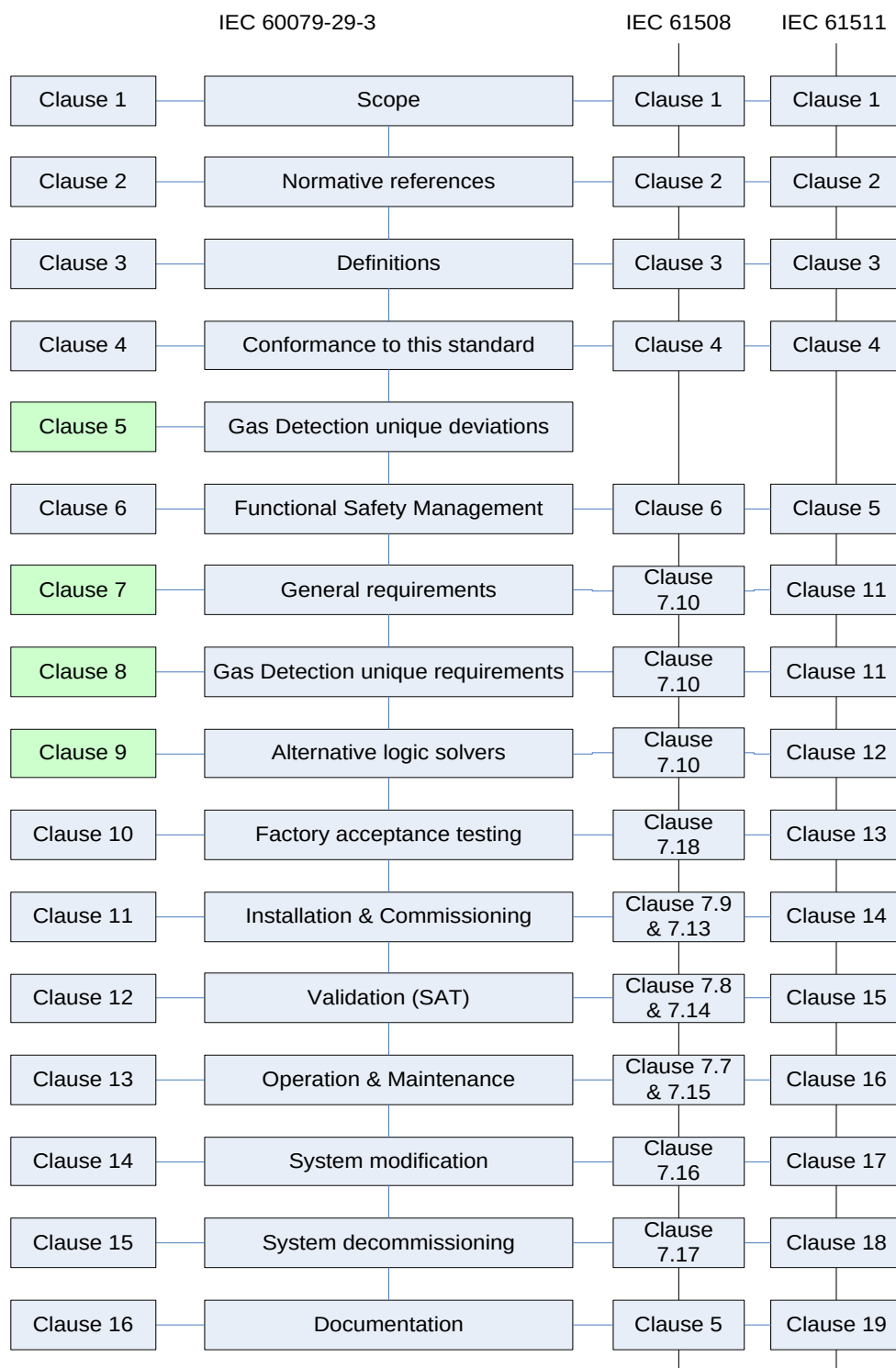
NOTE A motive force could be an electromechanical pump, air eductor or some other means to draw a sample gas, with a separate motive force for the purging of sample lines.

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 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*

SOMMAIRE

AVANT-PROPOS	51
INTRODUCTION.....	53
1 Domaine d'application	57
2 Références normatives	59
3 Termes et définitions	59
4 Exigences.....	61
4.1 Généralités	61
4.2 Taux de sollicitation	61
5 Caractéristiques spécifiques à la détection des gaz	61
5.1 Objectif	61
5.2 Caractéristiques.....	62
5.2.1 Généralités	62
5.2.2 Emplacement du capteur	62
5.2.3 Filtres de capteurs (passifs).....	62
5.2.4 Filtres de capteurs (actifs)	62
5.2.5 Principes des capteurs	63
5.2.6 Empoisonnement et réaction chimique défavorable	63
5.2.7 Durée de vie ppm.h ou %vol.h	63
5.2.8 Lectures négatives de gaz	63
5.2.9 Analyse des dangers et des risques.....	64
5.2.10 Efficacité préventive ou efficacité de réduction des impacts	64
5.2.11 Sensibilités croisées	64
5.2.12 Etats spéciaux	64
5.2.13 Normes métrologiques d'aptitude à la fonction	64
5.2.14 Gestion des signaux de défaut.....	65
5.2.15 Indication de dépassement	65
5.2.16 Étalonnage de substitution.....	65
5.2.17 Points de consigne d'alarme maximaux/minimaux.....	65
6 Gestion de la sécurité fonctionnelle	65
6.1 Objectif	65
6.2 Exigences	65
6.3 Compétence	67
7 Exigences générales	67
7.1 Objectifs	67
7.2 Exigences	67
7.2.1 Généralités	67
7.2.2 Fonctions relatives à la sécurité et non relatives à la sécurité	68
7.2.3 Fonctions de sécurité des différents objectifs d'intégrité	68
7.2.4 Comportement dans des conditions de défaillance dangereuse	68
7.2.5 Comportement dans des conditions de défaillance en sécurité	68
7.2.6 Comportement dans des conditions d'état spécial.....	69
7.2.7 Alimentation	69
7.2.8 Détecteur de gaz	70
7.2.9 Unité de commande de détection de gaz (unité logique)	70
7.2.10 Élément terminal (actionneur)	70

7.2.11	Indication visuelle	70
7.2.12	Sorties de commutation	71
7.2.13	Sorties de protocole.....	72
7.2.14	Entrées de protocole.....	73
7.2.15	Architecture système, valeurs PFD et PFH	73
8	Exigences uniques de détection de gaz	73
8.1	Objectifs	73
8.2	Exigences	74
8.2.1	Introduction à l'échantillonnage de gaz	74
8.2.2	Échantillonnage du gaz.....	74
8.2.3	Multiplexeur de gaz	75
8.2.4	Système de commande du multiplexeur de gaz	76
8.2.5	Conditionnement du gaz mesuré.....	76
8.2.6	Échantillonnage de gaz en mode diffusion	77
8.2.7	Étalonnage et ajustement automatiques	78
8.2.8	Système de commande de l'étalonnage et de l'ajustement automatiques	79
9	Unités de commande alternatives (unités logiques)	79
9.1	Objectifs	79
9.2	Exigences	79
9.2.1	Performances (métrologiques)	79
9.2.2	Programmation logique	80
10	Essais de réception en usine	80
10.1	Objectifs	80
10.2	Exigences	80
10.2.1	Planification	80
10.2.2	Réalisation	81
11	Installation et mise en service.....	81
11.1	Objectifs	81
11.2	Exigences	81
11.2.1	Planification.....	81
11.2.2	Réalisation	82
12	Validation du système.....	82
12.1	Objectifs	82
12.2	Exigences	83
12.2.1	Planification	83
12.2.2	Réalisation	83
13	Exploitation et maintenance.....	84
13.1	Objectifs	84
13.2	Exigences	84
13.2.1	Planification.....	84
13.2.2	Réalisation	84
14	Modification du système	85
14.1	Objectifs	85
14.2	Exigences	85
14.2.1	Planification.....	85
14.2.2	Réalisation	85
15	Déclassement / mise hors service du système	86

15.1	Objectifs	86
15.2	Exigences	86
15.2.1	Planification	86
15.2.2	Réalisation	86
16	Documentation	87
16.1	Objectifs	87
16.2	Exigences	87
Annexe A (informative) Applications typiques.....		88
A.1	Applications typiques de diffusion	89
A.1.1	Application 1.....	89
A.1.2	Application 2.....	90
A.1.3	Application 3.....	90
A.1.4	Application 4.....	90
A.2	Applications typiques d'échantillonnage	91
A.2.1	Échantillonnage point à point.....	91
A.2.2	Échantillonnage multiflux	92
Annexe B (informative) Références croisées entre normes		93
Annexe C (informative) Transformation des exigences.....		95
C.1	Généralités	95
C.2	Capacité SIL 1	95
C.2.1	Caractéristique	95
C.2.2	Transformation	95
C.3	Capacité SIL 2	96
C.3.1	Caractéristique	96
C.3.2	Transformation	96
C.4	Capacité SIL 3	96
C.4.1	Caractéristique	96
C.4.2	Transformation	96
Bibliographie.....		97
Figure 1 – Architecture d'un système de détection de gaz.....		55
Figure 2 – Normes connexes relatives aux systèmes instrumentés de sécurité		58
Figure A.1 – Boucles de sécurité de détection de gaz		90
Figure A.2 – Configurations typiques d'aspiration de détecteur de gaz.....		91
Figure B.1 – Références croisées entre normes.....		94
Tableau 1 – Descriptions des tâches types et articles les plus pertinents.....		56
Tableau 2 – Requête pour la gestion de la sécurité fonctionnelle (voir l'IEC 61508-1).....		66

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ATMOSPHÈRES EXPLOSIVES –

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

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60079-29-3 a été établie par le comité d'études 31 de l'IEC: Équipements pour atmosphères explosives.

La présente partie de l'IEC 60079-29 doit être utilisée conjointement avec les normes suivantes:

- IEC 60079-0, *Atmosphères explosives – Partie 0: Matériel – Exigences générales*
- IEC 60079-29-1, *Atmosphères explosives – Partie 29-1: Détecteurs de gaz – Exigences d'aptitude à la fonction des détecteurs de gaz inflammables*
- IEC 60079-29-2, *Atmosphères explosives – Partie 29-2: Détecteurs de gaz – Sélection, installation, utilisation et maintenance des détecteurs de gaz inflammables et d'oxygène*
- IEC 60079-29-4, *Atmosphères explosives – Partie 29-4: Détecteurs de gaz – Exigences d'aptitude à la fonction des détecteurs de gaz inflammables à chemin ouvert*

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
31/1105A/FDIS	31/1117/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 60079, sous le titre général: *Atmosphères explosives*, est disponible sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Les systèmes fixes de détection de gaz sont utilisés depuis de nombreuses années pour accomplir des fonctions instrumentées de sécurité. A l'instar de tout système instrumenté, un système fixe de détection de gaz comprend généralement une ou plusieurs entrées de détecteur de gaz, une unité de commande et un ou plusieurs éléments terminaux ou sorties. Des équipements périphériques supplémentaires peuvent être intégrés à un système fixe de détection de gaz, comme par exemple un système d'échantillonnage du gaz ou un système de conditionnement du gaz. Si un système fixe de détection de gaz, avec d'éventuels équipements périphériques utiles, est effectivement à utiliser pour accomplir des fonctions instrumentées de sécurité, il est essentiel que l'ensemble du système satisfasse à certaines normes minimales et à certains niveaux minimaux de performance.

Il est important de comprendre que le nombre de points de détection et leur emplacement approprié, leur redondance, la gestion de la maintenance régulière, notamment l'étalonnage ou la vérification des réponses et les autres caractéristiques spécifiques à la détection du gaz (comme la conception de systèmes d'échantillonnage du gaz) sont tous susceptibles d'avoir bien plus d'effet sur l'intégrité de l'ensemble du système instrumenté de sécurité (SIS – Safety Instrumented System) que le niveau exigé d'intégrité de sécurité (SIL – Safety Integrity Level) ou la capacité SIL d'une des unités fonctionnelles individuelles. Cependant cela n'exclut pas que les exigences correspondant à chaque fonction instrumentée de sécurité (SIF – Safety Instrumented Function) aient une intégrité fonctionnelle autonome.

La présente Norme internationale traite des normes minimales et des niveaux de performance correspondant à un système fixe de détection de gaz basé sur l'utilisation des systèmes électriques, électroniques ou électroniques programmables (système E/E/PE), pour toute application pour laquelle est indiqué un objectif de réduction du risque ou pour laquelle le système de détection de gaz sert de système de protection supplémentaire.

La présente Norme internationale ne s'applique pas aux détecteurs portables de gaz ou aux systèmes fixes de détection de gaz pour lesquels aucun objectif de réduction du risque n'est spécifié. Cependant, pour ces dispositifs ou systèmes, la présente Norme est susceptible d'être utilisée comme support aux bonnes pratiques.

Dans la présente Norme internationale, le terme "système de détection de gaz" est générique et s'applique aux détecteurs de gaz fixes autonomes, qui peuvent avoir leur propre niveau de déclenchement d'alarme interne et sorties de commutation jusqu'aux systèmes fixes de détection de gaz autonomes (Annexe A – Applications typiques).

La présente Norme internationale prend en compte l'éventuelle complexité de la chaîne d'approvisionnement que peut rencontrer le constructeur, le vendeur ou l'intégrateur système d'un dispositif de détection de gaz, comprenant sans toutefois s'y limiter:

- l'utilisation de détecteurs autonomes de gaz intégrés à un système de sécurité global par un constructeur, un vendeur ou un intégrateur système d'équipements de détection de gaz (ou équivalent);
- la conception et l'utilisation de sous-systèmes fixes de détection de gaz, comprenant d'éventuels équipements associés et/ou périphériques de détection de gaz intégrés à un système de sécurité global par un constructeur, un vendeur ou un intégrateur système d'équipements de détection de gaz (ou équivalent);
- la conception et l'utilisation d'un système fixe de détection de gaz complet, comprenant des équipements associés et/ou périphériques de détection de gaz, le tout constituant le système de sécurité global

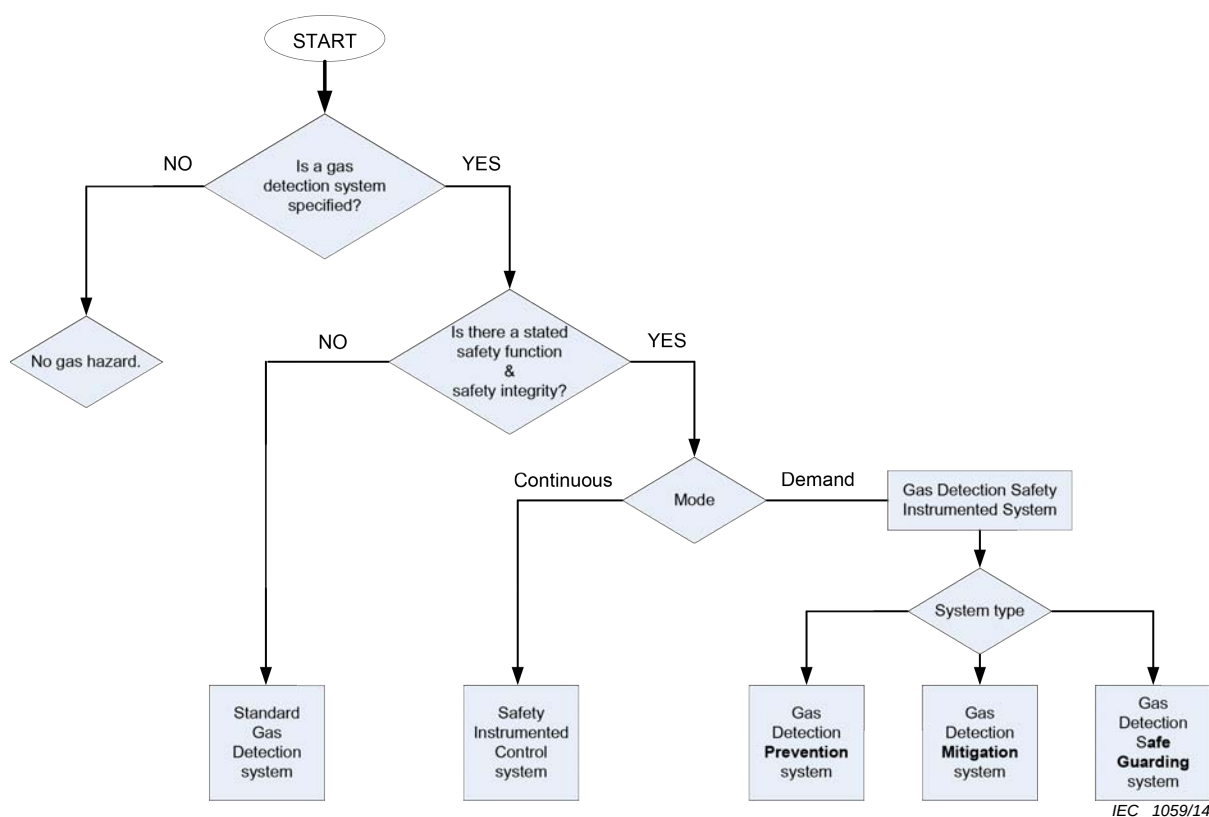
NOTE 1 Les parties 1, 2 et 3 de l'IEC 61508 traitent de la conception d'un détecteur de gaz autonome, de l'unité de commande ou de l'élément terminal. La présente Norme internationale fournit des recommandations sur la conception des équipements périphériques.

Avant de pouvoir appliquer la présente Norme internationale, il est important de comprendre et de classer l'application du système fixe de détection de gaz. Les trois applications principales sont les suivantes:

- en tant que système de prévention – l'ensemble du système ou une boucle instrumentée de régulation individuelle possède une fonction de sécurité et une intégrité de sécurité clairement définies.
- en tant que système de réduction des impacts – l'ensemble du système ou une boucle instrumentée de régulation individuelle possède une fonction de sécurité et une intégrité de sécurité clairement définies.
- en tant que système de protection supplémentaire – cette application concerne les systèmes fixes de détection de gaz ou les boucles instrumentées de régulation individuelles qui fonctionnent en parallèle (secondaire) à un système instrumenté de sécurité: le système fixe de détection de gaz ou la boucle instrumentée de régulation individuelle n'est utilisé que lorsque le système instrumenté de sécurité primaire ou une autre couche de protection ne fonctionne plus.

Il convient que l'utilisation d'un système de protection supplémentaire de détection de gaz ne contribue en aucun cas à la déclaration de tolérance aux anomalies du matériel (HFT – Hardware Fault Tolerance) pour le système instrumenté de sécurité.

Un système fixe de détection de gaz, comme indiqué à la Figure 1, peut fonctionner plusieurs fois par an en étant soumis à l'application; c'est pourquoi la présente Norme internationale admet qu'il convient de spécifier dans les exigences de sécurité le taux de sollicitation associé à "sur sollicitation" (faible sollicitation) (par exemple "> 1/an mais <10/an" peut être une référence).



Légende

Anglais	Français
Start	Début
No	Non

Anglais	Français
Yes	Oui
Is a gas detection system specified?	Un système de détection de gaz est-il spécifié?
No gas hazard	Aucun danger relatif au gaz
Is there a stated safety function & safety integrity?	Une fonction de sécurité & une intégrité de sécurité sont-elles spécifiées?
Standard Gas Detection system	Système normalisé de détection de gaz
Continuous	Continu
Mode	Mode
Demand	Sollicitation
Safety Instrumented Control system	Système de commande instrumenté de sécurité
Gas Detection Safety Instrumented System	Système instrumenté de sécurité de détection de gaz
System type	Type de système
Gas Detection Prevention system	Système de détection de gaz en prévention
Gas Detection Mitigation system	Système de détection de gaz en réduction des impacts
Gas Detection Safe Guarding system	Système de détection de gaz de protection supplémentaire

Figure 1 – Architecture d'un système de détection de gaz

Afin de mieux appréhender l'éventuelle complexité et les exigences uniques associées aux systèmes fixes de détection de gaz, un tel système peut être décomposé en unités fonctionnelles. La complexité de chaque unité fonctionnelle peut varier; il peut s'agir d'un simple détecteur de gaz ou d'une combinaison de composants formant un équipement périphérique. Chaque unité fonctionnelle est évaluée séparément par rapport à la présente Norme internationale et/ou à l'IEC 61508 au cours de la phase de conception initiale de l'unité fonctionnelle, ce qui permet d'obtenir les données de sécurité pour une unité fonctionnelle.

NOTE 2 Les éléments de base d'un sous-système/système (par exemple, un détecteur de gaz, un automate programmable à mémoire/une unité logique, etc.) sont considérés comme un produit, conformément aux parties 1, 2 et 3 de l'IEC 61508.

Chaque unité fonctionnelle est ensuite assemblée conformément à la présente Norme internationale afin de constituer un système fixe de détection de gaz complet. Il n'est pas nécessaire de réévaluer les unités fonctionnelles individuelles lorsqu'elles sont utilisées dans une configuration différente – il suffit d'évaluer la combinaison des unités fonctionnelles.

La présente Norme internationale est basée sur le modèle de cycle de vie de sécurité détaillé dans l'IEC 61508, mais elle apporte des informations supplémentaires et de soutien pour faciliter la réalisation des phases particulières du cycle de vie de sécurité considéré.

La présente Norme internationale spécifie dans la partie "Gestion de la sécurité fonctionnelle" les exigences auxquelles il convient que toutes les personnes ou sociétés impliquées dans la chaîne d'approvisionnement d'un système fixe de détection de gaz se conforment.

NOTE 3 La gestion de la sécurité fonctionnelle s'applique à toutes les phases du cycle de vie de sécurité, indépendamment du produit, du sous-système, de l'alimentation système ou du service fourni.

Pour le présent document, la capacité SIL exclut la prise en compte de la couverture de détection gaz ou le transport du gaz ou de la vapeur jusqu'au point de mesure – Ces deux sujets sont couverts par l'IEC 60079-29-2.

Le Tableau 1 donne une première idée de la pertinence des articles par rapport aux tâches types à accomplir.

Tableau 1 – Descriptions des tâches types et articles les plus pertinents

Applicable à	Définitions	Conformité à la présente Norme internationale	Caractéristiques spécifiques à la détection de gaz	Gestion de la sécurité fonctionnelle	Exigences générales	Exigences spécifiques à la détection de gaz	Unités de commande alternatives (unités logiques alternatives)	Essais de réception en usine	Installation et mise en service	Validation du système (SAT)	Fonctionnement et maintenance	Modification du système	Déclassement du système	Documentation
Article	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Consultant		+++		+++										
Prestataire		+++		+++										
Vendeur		+++		+++										
Intégrateur système		+++		+++										
Constructeur		+++		+++										
NOTE Chaque catégorie ci-dessus dispose de personnel dans plusieurs des catégories ci-dessous.														
Gestion générale	+	+	+		+	+	+	+	+	+	++	++	+	+
Ingénierie / gestion de la conception	+++	+	+++		+++	+++	+++	+	+	+	++	+++	++	++
Ingénierie / gestion du système	+++	+	+++		+++	+++	+++	+++	++	++	+	+++	++	++
Ingénierie / gestion de l'installation	++	+	++		+	++	+	+	+++	++	+	++	++	++
Ingénierie / gestion de la mise en service	++	+	++		++	++	+	+	+++	++	+	++	++	++
Ingénierie / gestion du service	++	+	++		++	++	+	+	++	++	+++	+++	+++	++
Ingénierie / gestion de la qualité	++	+	+++		+++	+++	+	+++	++	+++	+	++	+	+++
Agents de formation	+++	+	+++		+++	+++	++	+	+	+	+++	+	+	++
Fonctionnement & maintenance	+	+	++		+	++	+	++	+	+++	+++	+++	+++	+++
“+++” Le plus pertinent “++” Recommandé “+” Utile Il est nécessaire que l'utilisateur final, les autorités de réglementation et de certification connaissent toute la série de normes IEC 61508. NOTE Voir Annexe B pour des recommandations sur le cycle de vie de la détection de gaz.														

ATMOSPHÈRES EXPLOSIVES –

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

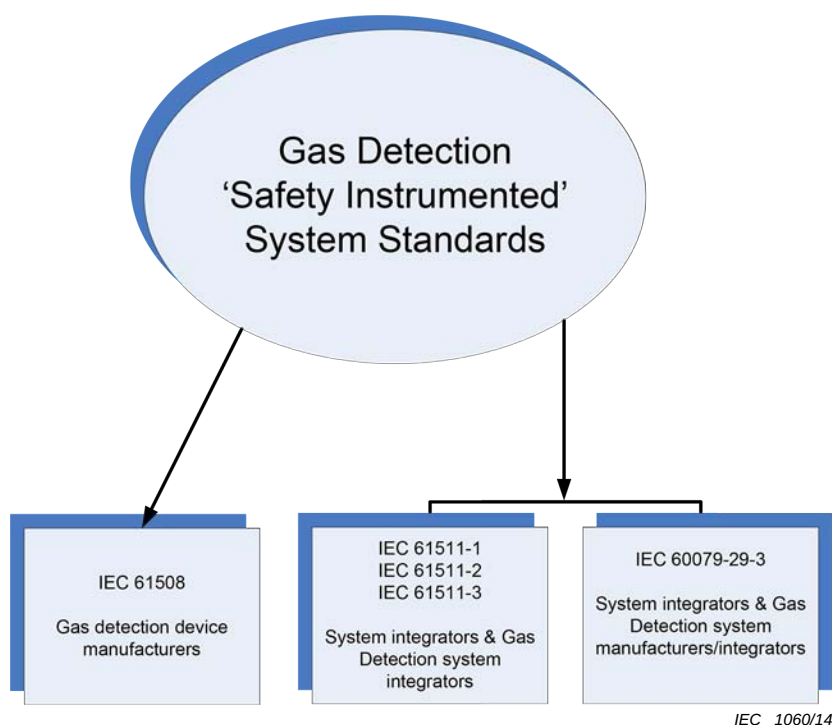
1 Domaine d'application

La présente Norme internationale donne des recommandations sur la conception et la mise en œuvre d'un système fixe de détection de gaz, comprenant des équipements associés et/ou périphériques de détection de gaz, permettant de détecter des gaz/vapeurs inflammables et de l'oxygène dans le cadre d'une application relative à la sécurité conformément à l'IEC 61508 et à l'IEC 61511. La présente Norme internationale s'applique aussi à la détection des gaz toxiques.

Les autres parties de la présente Norme internationale et les normes locales, nationales et internationales pertinentes spécifient séparément les exigences de performance d'un détecteur de gaz et d'une unité de commande de détection de gaz (unité logique). Ces normes sont généralement appelées Normes de Performances Métrologiques et traitent de la précision de la valeur mesurée, des performances globales du système, mais pas de l'intégrité du dispositif ou du système par rapport à la fonction de sécurité. La présente Norme internationale s'applique à l'intégrité de la fonction de sécurité.

NOTE Dans certaines juridictions, il est possible qu'il soit exigé qu'un Organisme de Certification certifie les performances des équipements utilisés pour la mesure des gaz inflammables, des vapeurs, des gaz toxiques et/ou de l'oxygène utilisés dans les applications de sécurité des personnes.

La présente Norme internationale formule des considérations relatives à la sécurité des systèmes fixes de détection de gaz, comprenant des équipements associés et/ou périphériques de détection de gaz, en termes du cadre et de philosophie de l'IEC 61508 et introduit les exigences particulières requises par un système fixe de détection de gaz, comme indiqué à la Figure 2.



Légende

Anglais	Français
Gas Detection "Safety Instrumented" System Standards	Normes relatives aux systèmes "instrumentés de sécurité" de détection des gaz
Gas detection device manufacturers	Constructeurs de dispositifs de détection de gaz
System integrators & Gas Detection system integrators	Intégrateurs de système & intégrateurs de système de détection de gaz
System integrators & Gas Detection system manufacturers/integrators	Intégrateurs de système & intégrateurs/constructeurs de système de détection de gaz

Figure 2 – Normes connexes relatives aux systèmes instrumentés de sécurité

La présente Norme internationale ne prend pas en compte le niveau d'intégrité de sécurité SIL 4. On considère qu'il serait irréaliste de vouloir atteindre le niveau SIL 4 pour les systèmes de détection de gaz.

NOTE 3 Une étude de risque ne détermine que rarement une intégrité de sécurité supérieure à SIL 2 pour un système fixe de détection de gaz.

La présente Norme internationale s'applique aux systèmes fixes de détection de gaz qui peuvent être constitués des unités fonctionnelles matérielles suivantes:

- un capteur de gaz/transmetteur;
- une unité de commande de détection de gaz (unité logique);
- un dispositif d'échantillonnage de gaz (flux unique et multiplex);
- un dispositif de conditionnement de gaz;
- un dispositif d'étalonnage et d'ajustement automatique de gaz;
- un module de sortie (s'il n'est pas intégré à l'unité de commande).

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60079-29-1, *Atmosphères explosives – Partie 29-1: Détecteurs de gaz – Exigences d'aptitude à la fonction des détecteurs de gaz inflammables*

IEC 60079-29-2:2007, *Atmosphères explosives – Partie 29-2: Détecteurs de gaz – Sélection, installation, utilisation et maintenance des détecteurs de gaz inflammables et d'oxygène*

IEC 60079-29-4, *Atmosphères explosives – Partie 29-4: Détecteurs de gaz – Exigences d'aptitude à la fonction des détecteurs de gaz inflammables à chemin ouvert*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-1, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1

système de protection supplémentaire

système fixe de détection de gaz ou boucles instrumentées de régulation individuelles qui fonctionnent en parallèle (secondaire) à un système instrumenté de sécurité: le système fixe de détection de gaz ou la boucle instrumentée de régulation individuelle ne sont utilisés que lorsque le système instrumenté de sécurité primaire ou une autre couche de protection ne fonctionne plus

3.2

équipement associé de détection de gaz

équipement complémentaire de l'équipement de détection de gaz couvert par l'IEC 60079-29-1 ou l'IEC 60079-29-4 qui fait partie de l'ensemble du système fixe de détection de gaz et qui est essentiel par rapport à la fonction de sécurité

Note 1 à l'article: Les équipements associés de détection de gaz sont par exemple l'échantillonnage de gaz ou le multiplexage de gaz.

3.3

défaillance dangereuse

défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

Note 1 à l'article: Le fait que cette potentialité se réalise ou non est susceptible de dépendre de l'architecture de canal du système; pour les systèmes ayant des canaux multiples/redondants destinés à accroître la sécurité, il est

moins probable qu'une défaillance dangereuse du matériel conduise à un état dangereux de l'ensemble ou à un état dans lequel la fonction ne peut plus être exécutée.

Note 2 à l'article: La perte d'une tête de détection est un exemple de défaillance dangereuse.

3.4

mode de sécurité intrinsèque

mode de signal de sortie dans lequel le fonctionnement normal est le mode sous tension.

Note 1 à l'article: En cas de perte de l'alimentation électrique, la sortie sera mise hors tension et le signal sera actif.

3.5

signal de défaut

sortie audible, visible ou d'un autre type, différente du signal d'alarme, permettant, directement ou indirectement, un avertissement ou une indication de dysfonctionnement du matériel

3.6

unité fonctionnelle

entité de matériel ou de logiciel, ou les deux à la fois, capable d'assurer une fonction déterminée qui peut comprendre plusieurs éléments

3.7

module matériel

entité de matériel capable d'assurer une fonction déterminée, par exemple un transmetteur ou une unité de commande

3.8

point de mesure

emplacement d'un détecteur de gaz

3.9

équipement périphérique

équipement qui fait partie de l'ensemble du système fixe de détection de gaz mais qui n'est généralement pas essentiel par rapport à la fonction de sécurité

Note 1 à l'article: Le stockage des données est un exemple d'équipement indépendant de la fonction de sécurité.

3.10

essai périodique

essai périodique destiné à détecter les défaillances cachées d'un système relatif à la sécurité de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition "comme neuf" ou dans une condition aussi proche que possible de celle-ci

3.11

défaillance en sécurité

défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

Note 1 à l'article: Une défaillance en sécurité est par exemple un défaut d'un circuit de filtrage CEM qui n'a pas de conséquence en fonctionnement normal mais qui peut déclencher une alarme parasite en cas de perturbations CEM.

3.12

état de sécurité

état de l'équipement commandé (EUC – equipment under control) lorsque la sécurité est réalisée

Note 1 à l'article: Pendant son évolution depuis un état potentiellement dangereux vers un état de sécurité final, l'EUC est susceptible de passer par un certain nombre d'états de sécurité intermédiaires. Dans certaines

situations, l'état de sécurité n'est atteint que durant le temps où l'EUC est continuellement commandé. Cette commande continue est susceptible de s'étendre sur une période courte ou indéfinie.

3.13

ligne d'échantillonnage

tuyau ou tube dédié qui connecte un point d'échantillonnage à un détecteur de gaz dans un système d'échantillonnage point à point ou multiflux

3.14

point d'échantillonnage

extrémité d'une ligne d'échantillonnage à laquelle est prélevé le gaz

Note 1 à l'article: Un point d'échantillonnage (matériel) comprend normalement un boîtier physique contenant un filtre à particules ou équivalent.

3.15

capacité SIL

caractéristique des unités fonctionnelles conformes aux exigences de l'IEC 61508-2 et de l'IEC 61508-3, appropriées pour une utilisation dans des fonctions respectivement de niveau SIL 1, 2 ou 3 alloué

3.16

état spécial

état du matériel autre que celui pour lequel la surveillance de la concentration de gaz est active, par exemple le préchauffage, les modes d'étalonnage ou les défauts

4 Exigences

4.1 Généralités

Il convient de s'assurer que chacune des exigences spécifiées des Articles 5 à 16 ont été satisfaites selon les critères définis et que le ou les objectifs des articles ont donc été atteints.

4.2 Taux de sollicitation

Un système fixe de détection de gaz peut fonctionner plusieurs fois par an en étant soumis à l'application; c'est pourquoi la présente Norme internationale admet qu'il convient de spécifier dans les exigences de sécurité le taux de sollicitation associé à "sur sollicitation" (faible sollicitation) (par exemple "> 1/an mais <10/an" peut être une référence).

Les intervalles entre les essais périodiques pour le mode faible sollicitation sont déterminés en supposant que le taux de sollicitation est d'1 par an au maximum.

Si le taux de sollicitation spécifié est supérieur à 1 par an par le facteur "X", l'intervalle entre les essais périodiques doit être réduit par le facteur "X".

5 Caractéristiques spécifiques à la détection des gaz

5.1 Objectif

L'objectif de l'Article 5 est d'identifier les caractéristiques spécifiques qui s'appliquent aux systèmes fixes de détection de gaz par rapport aux autres éléments sensibles, aux systèmes instrumentés de commande et aux actionneurs.

5.2 Caractéristiques

5.2.1 Généralités

Les systèmes fixes de détection de gaz sont différents des systèmes instrumentés normalisés sous bien des aspects. Pour tout système fixe de détection de gaz, il est nécessaire, au cours de la phase de conception et d'ingénierie, de comprendre les caractéristiques et/ou les sollicitations spécifiques associées à la détection de gaz. Les Paragraphes 5.2.2 à 5.2.17 en détaillent les principales différences.

NOTE Voir l'IEC 60079-29-2 pour des lignes directrices sur la sélection, l'installation, l'utilisation et la maintenance des détecteurs de gaz inflammables et d'oxygène. Ce document donne des informations supplémentaires applicables à bon nombre des paragraphes de l'Article 8 de l'IEC 60079-29-2:2007.

5.2.2 Emplacement du capteur

Les systèmes de détection de gaz reposent sur un mécanisme de transport permettant de déplacer la fuite de gaz/la vapeur vers l'élément sensible, contrairement aux dispositifs de sécurité de processus, tels que les capteurs de pression et de température, qui sont en contact direct avec le processus.

Ainsi, la détermination de l'emplacement du point de détection final n'est pas couverte par la présente Norme. Cependant, il convient de noter que l'emplacement du point de détection peut avoir un effet global sur le fonctionnement d'un système fixe de détection de gaz, que le système soit relatif à la sécurité ou non.

NOTE 1 Voir l'IEC 60079-29-2 pour des lignes directrices sur l'emplacement du capteur. Dans le présent document, on part du principe que le gaz ou la vapeur atteint le capteur.

NOTE 2 Voir l'IEC 60079-10-1 pour des indications sur la classification de zone.

NOTE 3 Par exemple, voir l'ISA-TR84.00.07 pour des lignes directrices sur l'évaluation de l'efficacité du système de détection de gaz.

5.2.3 Filtres de capteurs (passifs)

Les capteurs de gaz peuvent comporter un filtre passif destiné à protéger la membrane du capteur contre la poussière, la saleté ou l'humidité ambiante, ou un disque métallique fritté de protection contre l'explosion. Tous les types de filtres passifs ont un mode de défaillance non détecté dangereux (par exemple, blocage) et exigent donc de procéder à une inspection planifiée et des essais périodiques.

Il convient que la fonction de sécurité définie par point de détection prenne en compte l'utilisation intrinsèque de ces filtres passifs et comprenne donc dans la fonction de sécurité définie un temps de réponse acceptable au début d'un essai périodique.

5.2.4 Filtres de capteurs (actifs)

Les capteurs de gaz peuvent comporter un filtre actif destiné à conditionner ou modifier le gaz ou la vapeur détecté(e). Il convient que ces filtres actifs soient spécifiés par le constructeur; ces filtres ont une durée de vie définie. Tous les filtres de ce type ont des modes de défaillance non détectés dangereux (par exemple, blocage, saturation et désactivation) et exigent donc de procéder à une inspection planifiée et des essais périodiques.

Les capteurs de gaz peuvent comporter un filtre catalytique. Ces filtres n'ont pas de durée de vie définie mais ils sont sujets aux mêmes effets que les filtres passifs. Il convient de traiter ces filtres comme des filtres passifs, à moins que les conditions environnementales n'affectent le matériau du catalyseur. Tous les filtres de ce type ont un mode de défaillance non détecté dangereux et exigent donc de procéder à une inspection planifiée et des essais périodiques.

5.2.5 Principes des capteurs

Il convient d'évaluer tous les principes de mesure du capteur par rapport à l'adéquation de l'application. En fonction de l'application et des principes, les capteurs peuvent être:

- empoisonnés – incapables de détecter le gaz cible;
- inhibés – moins sensibles ou incapables de détecter le gaz cible;
- saturés – incapables d'effectuer correctement les mesures en raison d'un contact excessif avec le gaz cible;

NOTE Il s'agit généralement d'un effet temporaire;

- consommés – moins sensibles ou incapables de détecter le gaz cible car la vie utile du capteur a été consommée;
- déshydratés – modification de la sensibilité ou de la précision;
- hydratés – modification de la sensibilité ou de la précision;
- sujets à l'effet d'endormissement – incapables de détecter des changements de faible concentration;
- sujets à une interférence optique – sujets à des lectures de gaz parasites;
- sujets à un blocage optique – incapables de détecter le gaz cible.

Certains de ces états du capteur peuvent être détectés par diagnostics, ainsi toute défaillance est "détectée comme dangereuse". D'autres états du capteur ne peuvent pas être détectés par diagnostics, ainsi toute défaillance est "non détectée comme dangereuse" ce qui nécessite de ce fait de procéder à une inspection planifiée et des essais périodiques du capteur (étalonnage).

5.2.6 Empoisonnement et réaction chimique défavorable

Les technologies particulières des capteurs sont sujettes aux défaillances de mode commun; les substances en suspension de l'air peuvent inhiber ou empoisonner certaines technologies de capteur (par exemple les capteurs catalytiques) alors que les capteurs électrochimiques peuvent être sujets à des réactions chimiques défavorables.

Les capteurs utilisant ces technologies ont un mode de défaillance non détecté dangereux (spécifique à l'application) à moins que les diagnostics des capteurs ne détectent une perte de sensibilité des capteurs. Si pour une application, l'empoisonnement et/ou des réactions chimiques défavorables ne peuvent être exclus, une inspection planifiée et des essais périodiques du capteur (étalonnage) sont exigés.

Si ces modes de défaillance ne peuvent être exclus pour une application, les capteurs n'amélioreront pas le niveau d'intégrité de sécurité car il s'agit de défaillances d'origine commune. L'intégrité de sécurité sera améliorée dans ces cas uniquement par l'application de divers principes de détection.

5.2.7 Durée de vie ppm.h ou %vol.h

Les technologies particulières des capteurs ont une durée de vie ppm.h ou %vol.h. Les capteurs à durée de vie limitée peuvent avoir un mode de défaillance non détecté dangereux; une inspection planifiée et des essais périodiques du capteur (étalonnage) sont donc exigés, à moins que les diagnostics ne détectent l'amorce de fin de vie du capteur.

5.2.8 Lectures négatives de gaz

Contrairement aux mesures de processus, les capteurs de gaz n'ont pas de lectures négatives de valeurs de gaz.

NOTE Les signaux inférieurs à zéro sont susceptibles d'être causés par une dérive de zéro ou des sensibilités croisées défavorables.

5.2.9 Analyse des dangers et des risques

Les gaz et les vapeurs provoquent de nombreux dangers. Ils peuvent être inflammables, toxiques ou les deux. Les niveaux d'oxygène peuvent être trop élevés ou insuffisants. Il convient que toute analyse des dangers et des risques prenne en compte tous les dangers associés aux gaz et aux vapeurs, ce qui inclut les effets à court et à long termes. Il convient que la dispersion des gaz comprenne la modélisation en prenant en compte les densités relatives des gaz/vapeurs. Il convient de prendre en considération les conditions environnementales, y compris la présence d'autres gaz.

NOTE Pour de plus amples informations, voir l'IEC 60079-29-2.

5.2.10 Efficacité préventive ou efficacité de réduction des impacts

Certaines fonctions de détection de gaz sont préventives alors que d'autres ne font que réduire les conséquences du dégagement. Ces fonctions de réduction peuvent ne pas être totalement efficaces, même lorsqu'elles sont activées. La détermination de l'efficacité de la fonction de réduction n'est pas couverte par le domaine d'application de la présente Norme internationale mais dépend plutôt du fonctionnement et du personnel spécifiques à l'installation.

5.2.11 Sensibilités croisées

La plupart des capteurs de détection de gaz sont sujets aux sensibilités croisées qui peuvent augmenter ou diminuer la réponse au gaz. De manière générale, les sensibilités croisées peuvent déclencher des alarmes parasites ou empêcher le déclenchement d'alarmes. Il convient donc d'accorder une attention particulière aux éventuels dégagements de gaz ou de vapeurs d'une application.

5.2.12 Etats spéciaux

Les systèmes de détection de gaz utilisent des signaux d'états spéciaux pour indiquer l'état des points de mesure uniques, des boucles de régulation individuelles ou de l'ensemble du système. Les états spéciaux peuvent indiquer les conditions suivantes:

- le point de mesure, la boucle de régulation ou le système est en mode démarrage;
- le point de mesure, la boucle de régulation ou le système est inhibé/neutralisé;
- étalonnage du point de mesure, de la boucle de régulation ou du système;
- autres états du système empêchant la surveillance de la concentration de gaz.

Les états spéciaux déclenchent un contact ou autre signal de sortie transmissible. L'utilisation de ces signaux d'états spéciaux doit être clairement définie dans la fonction de sécurité définie et il n'est pas toujours nécessaire de lancer un "état de sécurité" dans une condition d'état spécial.

NOTE L'IEC 60079-29-1 exige des signaux d'états spéciaux.

5.2.13 Normes métrologiques d'aptitude à la fonction

La conformité aux normes métrologiques d'aptitude à la fonction est exigée pour tous les niveaux SIL.

NOTE Les normes de performances métrologiques internationales comprennent l'IEC 60079-29-1 et l'IEC 60079-29-4. D'autres normes sont susceptibles de s'appliquer dans certaines juridictions, notamment les normes relatives à la détection de gaz toxique et d'oxygène.

Les normes de performances métrologiques comprennent les essais de compatibilité électromagnétique (CEM) suivant l'IEC 61326-1. Il convient de prendre en compte la CEM de manière similaire pour l'équipement de détection de gaz associé.

5.2.14 Gestion des signaux de défaut

La gestion des signaux de défaut doit être clairement définie dans la fonction de sécurité définie. Contrairement aux systèmes d'arrêt de processus, la sortie souhaitée d'un système fixe de détection de gaz peut être de ne pas générer un faux processus d'arrêt (déclenchement parasite) ou d'évacuation.

5.2.15 Indication de dépassement

Lorsqu'une application utilise une technologie de capteur catalytique, elle doit générer un affichage (lecture) sans ambiguïté pour une mesure de dépassement.

NOTE Il s'agit d'une exigence de l'IEC 60079-29-1.

5.2.16 Étalonnage de substitution

Lorsqu'un gaz cible n'est pas disponible pour réaliser l'étalonnage du capteur de gaz, il est possible d'utiliser un gaz de substitution. Les étalonnages avec des gaz de substitution seront moins précis. Il convient que les étalonnages avec des gaz de substitution soient réalisés selon les recommandations du constructeur et qu'ils soient clairement identifiés dans le manuel de sécurité du système associé.

La sensibilité relative du gaz de substitution est susceptible de varier en fonction de la température, de l'humidité, du vieillissement, etc. De même, les temps de réponse et les temps de recouvrement du gaz de substitution peuvent différer considérablement de ceux du gaz cible. Ces conditions sont susceptibles d'avoir une influence sur les essais périodiques.

5.2.17 Points de consigne d'alarme maximaux/minimaux

En fonction de l'application, il peut être recommandé de ne pas régler les alarmes au-delà d'un certain pourcentage de l'étendue de mesure.

Afin de prévenir des déclenchements parasites dus à la dérive du capteur, il convient de définir un point de consigne d'alarme minimal.

6 Gestion de la sécurité fonctionnelle

6.1 Objectif

L'objectif de cet article est de définir les exigences minimales de gestion de la sécurité fonctionnelle auxquelles tout individu, service ou organisation doit satisfaire en fonction de ses responsabilités au cours de toute phase du cycle de vie d'un système fixe de détection de gaz.

6.2 Exigences

Un système de gestion de la sécurité fonctionnelle doit être établi au cours de chaque phase du cycle de vie du système fixe de détection de gaz. Un système de gestion de la sécurité fonctionnelle doit prendre en compte les points suivants:

- la fonction de sécurité et le niveau d'intégrité de sécurité;
- le caractère unique de l'application ou de la conception;
- les organisations impliquées dans l'ensemble du cycle de vie;
- l'étendue de la fourniture pour chaque organisation.

NOTE La rigueur d'un système de gestion de la sécurité fonctionnelle peut changer en fonction du niveau d'intégrité défini.

Tout individu, service ou organisation impliqué dans une ou plusieurs phases du cycle de vie d'un système fixe de détection de gaz doit, en fonction des phases correspondant à ses responsabilités globales, spécifier toutes les activités de gestion et d'ordre technique qui sont nécessaires pour garantir que le système fixe de détection de gaz réalise et maintient la fonction et l'intégrité de sécurité fonctionnelle exigées.

Tout individu, service ou organisation responsable de l'exécution et de la revue de chacune des phases du cycle de vie de sécurité doit être identifié et informé par écrit des responsabilités qui lui sont assignées.

Tout individu, service ou organisation impliqué dans les activités du cycle de vie de sécurité doit être compétent pour conduire les activités dont il est responsable. Une attention particulière doit être portée aux points suivants:

- la connaissance et l'expérience des systèmes fixes de détection de gaz et des normes locales, nationales et internationales pertinentes relatives à la détection de gaz;
- la connaissance et l'expérience des systèmes fixes de détection de gaz lorsqu'ils sont utilisés en tant que systèmes de protection primaire;
- la connaissance et l'expérience de l'utilisation, du fonctionnement et de la maintenance des systèmes fixes de détection de gaz.

Tout individu, service ou organisation impliqué dans une ou plusieurs phases du cycle de vie d'un système fixe de détection de gaz doit mettre en place la planification de la sécurité qui définit les activités dont l'exécution est exigée pour garantir l'obtention et le maintien de la fonction de sécurité et de l'intégrité de sécurité. Des plans de sécurité doivent être mis à jour le cas échéant.

Tout individu, service ou organisation impliqué dans l'analyse des dangers et des risques associée au système fixe de détection de gaz doit déterminer à la fois les effets instantanés d'un dégagement de gaz et les effets à long terme et cachés associés à un dégagement de gaz.

Le constructeur du système ou du sous-système fixe de détection de gaz ou du détecteur de gaz est responsable des aspects de commercialisation du système ou du sous-système fixe de détection de gaz ou du détecteur de gaz. La responsabilité doit non seulement s'appliquer à la conception, à la construction et à la production mais doit aussi couvrir les informations exigées pour l'utilisation prévue du système ou du sous-système fixe de détection de gaz ou du détecteur de gaz.

Une revue indépendante est exigée pour tous les objectifs SIL et l'augmentation du degré d'indépendance doit correspondre à l'augmentation du nombre d'objectifs SIL. Le Tableau 2 indique les exigences de rigueur à appliquer à la gestion de la sécurité fonctionnelle en fonction de l'objectif SIL. Lorsque plusieurs objectifs SIL correspondent à différentes boucles de régulation, la rigueur et l'indépendance doivent se conformer à l'objectif SIL le plus élevé pour l'ensemble du système fixe de détection de gaz.

Tableau 2 – Requête pour la gestion de la sécurité fonctionnelle (voir l'IEC 61508-1)

	Pas de SIL (0)	SIL 1	SIL 2	SIL 3
Fournisseur de détecteur de gaz	C	C	HR	O
Fournisseur du sous-système C	C	HR	O	O
Fournisseur du système de détection de gaz	C	O	O	O
Intégrateur système ou équivalent	C	O	O	O
C = Conseillé, HR = Hautement Recommandé, O = Obligatoire				

6.3 Compétence

La compétence est la capacité à assumer des responsabilités et à effectuer des activités conformément à une norme reconnue, régulièrement. La compétence est une combinaison de connaissances pratiques et intellectuelles, d'expérience et de savoir. Il convient que toutes les organisations impliquées dans une ou plusieurs phases du cycle de vie d'un système fixe de détection de gaz mettent en œuvre un plan de gestion de la compétence. Il convient qu'un tel plan de gestion de la compétence apporte des preuves montrant que tous les individus sont compétents pour effectuer les activités dont ils ont la charge. Lors de l'évaluation de la compétence des individus, il convient de traiter au moins les points suivants:

- les connaissances d'ingénierie, la formation et l'expérience, adaptées à la phase dont ils ont la charge;
- les connaissances d'ingénierie, la formation et l'expérience, adaptées à la technologie (notamment logicielle) utilisée;
- les connaissances d'ingénierie, la formation et l'expérience, adaptées à la complexité et à la nouveauté de la conception du système fixe de détection de gaz;
- les connaissances d'ingénierie, la formation et l'expérience, adaptées à l'application ou à l'utilisation du système fixe de détection de gaz;
- les connaissances des exigences légales et réglementaires concernant la sécurité;
- la gestion adéquate et les qualités de commandement appropriées à leur rôle dans les activités du cycle de vie de sécurité;
- les connaissances et la formation dans le domaine des normes locales, nationales et internationales appropriées et applicables aux systèmes fixes de détection de gaz, aux systèmes instrumentés de sécurité et aux systèmes de qualité pertinents, notamment les normes indiquées à l'Article 2 de la présente Norme internationale;
- la compréhension des conséquences potentielles d'une défaillance;
- la formation à la détection de gaz et à la réponse en cas d'urgence en zone dangereuse, afin de garantir que les actions des individus ne réduisent pas l'efficacité du système de détection de gaz ou ne créent pas d'autres problèmes de sécurité dans l'installation;
- l'expérience acquise et sa pertinence par rapport aux tâches spécifiques à effectuer;
- la formation ou la compétence en évaluation SIL pour les systèmes de contrôle.

La formation, l'expérience et les qualifications de tous les individus impliqués dans toute phase du cycle de vie d'un système fixe de détection de gaz doivent être documentées.

7 Exigences générales

7.1 Objectifs

L'objectif de l'Article 7 est de définir les exigences générales pour un système fixe de détection de gaz.

7.2 Exigences

7.2.1 Généralités

La conception d'un système fixe de détection de gaz doit être conforme à la spécification définie des exigences de sécurité et prendre en compte toutes les exigences du présent article.

L'utilisation et la combinaison d'un détecteur de gaz (incluant le capteur), d'une unité de commande et d'un élément terminal doivent suivre la présente norme en plus de l'IEC 61508.

Pour les industries de transformation, l'IEC 61511 peut être utilisée.

Un système fixe de détection de gaz doit être conçu pour garantir la facilité de réalisation des activités d'exploitation, de maintenance et d'essai.

Il convient que l'action d'un système fixe de détection de gaz en état spécial ou en condition d'alarme activée par le gaz ne passe pas automatiquement à un état de sécurité.

7.2.2 Fonctions relatives à la sécurité et non relatives à la sécurité

Un système fixe de détection de gaz est susceptible de mettre en œuvre des fonctions relatives à la sécurité et non relatives à la sécurité. La spécification des exigences de sécurité définit clairement quelles fonctions du système fixe de détection de gaz ont un niveau d'intégrité de sécurité alloué. Lorsque le système fixe de détection de gaz est tenu de mettre en œuvre des fonctions relatives à la sécurité et non relatives à la sécurité, le matériel et le logiciel qui peuvent avoir un effet préjudiciable sur une fonction de sécurité en fonctionnement normal et en conditions de défaut doivent être conformes au niveau d'intégrité de sécurité le plus élevé.

NOTE Il est souhaitable de séparer les fonctions de sécurité et les fonctions non relatives à la sécurité, dans toute la mesure du possible.

7.2.3 Fonctions de sécurité des différents objectifs d'intégrité

Lorsqu'un système fixe de détection de gaz est tenu de mettre en œuvre des fonctions de sécurité de différents niveaux d'intégrité de sécurité, tout le matériel et le logiciel doivent être conformes au niveau d'intégrité de sécurité le plus élevé, à moins de pouvoir démontrer que la fonction de sécurité des niveaux inférieurs d'intégrité de sécurité ne peut avoir d'effet préjudiciable sur la fonction de sécurité des niveaux plus élevés d'intégrité de sécurité.

7.2.4 Comportement dans des conditions de défaillance dangereuse

Exigences:

Toutes les capacités SIL:

Dans un système fixe de détection de gaz avec ou sans redondance, la détection d'une défaillance dangereuse (par essai de diagnostic, essai périodique ou tout autre moyen) doit faire référence à la spécification des exigences de sécurité et avoir pour résultat l'initiation:

- a) d'une action spécifiée permettant d'atteindre un état de sécurité; ou
- b) d'une action spécifiée signalant le défaut à l'opérateur qui peut lancer une action pour atteindre un état de sécurité; ou
- c) d'une action spécifiée signalant le défaut à l'opérateur qui lance une action de réparation de sorte que la fonction de sécurité soit disponible dans l'intervalle du temps moyen de rétablissement (MTTR) spécifié; ou
- d) d'une combinaison de a), b) ou c).

La spécification des exigences de sécurité doit spécifier clairement l'acceptabilité des déclenchements parasites ou l'indisponibilité du système lorsqu'un défaut est détecté.

Si la fonction de sécurité ne peut être réparée ou rétablie dans l'intervalle du temps moyen de rétablissement, l'utilisateur final est alors responsable de l'initiation des actions supplémentaires de réduction du risque. Il convient de détailler les autres actions de réduction du risque dans la spécification des exigences de sécurité.

7.2.5 Comportement dans des conditions de défaillance en sécurité

Exigences:

Toutes les capacités SIL:

Dans un système fixe de détection de gaz avec ou sans redondance, la détection d'une défaillance en sécurité (par essai de diagnostic, essai périodique ou tout autre moyen) doit faire référence à la spécification des exigences de sécurité et avoir pour résultat l'initiation:

- a) d'une action spécifiée signalant le défaut à l'opérateur qui lance une action de réparation; ou
- b) d'une action spécifiée signalant le défaut à l'opérateur qui peut lancer une action pour atteindre un état de sécurité; ou
- c) d'une action spécifiée permettant d'atteindre un état de sécurité; ou
- d) d'une combinaison de a), b) ou c).

NOTE La réponse aux défaillances en sécurité est susceptible de ne pas exiger d'action immédiate, et la réponse aux défaillances en sécurité dépend fortement de la nature de la défaillance.

7.2.6 Comportement dans des conditions d'état spécial

Exigences:

Toutes les capacités SIL:

Des états spéciaux autres que des défauts sont lancés intentionnellement. Les actions à entreprendre sont spécifiques à l'application et doivent donc être spécifiées dans le manuel de sécurité.

Dans un système fixe de détection de gaz avec ou sans redondance, la détection d'un état spécial doit faire référence à la spécification des exigences de sécurité et avoir pour résultat l'initiation:

- a) d'une action spécifiée signalant l'état spécial à l'opérateur qui lance une étude de façon à quitter l'état spécial et à relancer ou à rendre disponible la fonction de sécurité dans l'intervalle du temps moyen de rétablissement (MTTR); ou
- b) d'une action spécifiée signalant l'état spécial à l'opérateur qui peut lancer une action pour atteindre un état de sécurité; ou
- c) d'une action spécifiée permettant d'atteindre un état de sécurité; ou
- d) d'une combinaison de a), b) ou c).

7.2.7 Alimentation

7.2.7.1 Caractérisation

Les alimentations ne sont pas incluses dans la caractérisation de la fonction de sécurité lorsque l'ensemble du système fixe de détection de gaz est prévu pour fonctionner en mode de sécurité intrinsèque pour toutes les sorties relatives à une condition de défaut.

Si les sorties de sécurité intrinsèque ne sont pas utilisées au sein du système fixe de détection de gaz, il convient d'inclure la fiabilité du système d'alimentation dans la caractérisation de la fonction de sécurité.

7.2.7.2 Exigences

Toutes les capacités SIL:

- a) Système à alimentation unique: un signal de défaut doit être initié en cas de défaillance de l'alimentation.
- b) Système à alimentation redondante: aucune perte de la fonction de sécurité ne doit se produire pendant la transition d'un système d'alimentation à un autre. Il convient d'initier une indication en cas de défaillance d'une des deux alimentations. Il convient d'initier un signal de défaut en cas de défaillance des deux alimentations.

- c) Système muni d'une alimentation sans interruption (ASI): aucune perte de la fonction de sécurité ne doit se produire pendant la transition du système d'alimentation à l'ASI. Il convient d'initier une indication en cas de défaillance de l'alimentation et si le système fixe de détection de gaz passe en alimentation ASI. La fonction de sécurité du système doit décrire les mesures opérationnelles nécessaires lorsque le système fixe de détection de gaz est alimenté par un système ASI à alimentation par batterie (durée limitée). Il convient d'initier un signal de défaut en cas de défaillance du système ASI.

Le système fixe de détection de gaz doit être capable de surveiller l'alimentation en courant continu. Si la tension en courant continu augmente ou chute au-delà des limites prédéfinies, un état spécial doit être signalé.

7.2.8 Détecteur de gaz

Exigences:

Toutes les capacités SIL:

Un détecteur de gaz, y compris le capteur, étant un élément de production normalisé vendu par le constructeur, un détecteur de gaz, y compris le capteur, doit par conséquent être conforme aux IEC 61508-1, IEC 61508-2 et IEC 61508-3.

Un détecteur de gaz, y compris le capteur, doit être conforme aux normes métrologiques de performance applicables (voir IEC 60079-29-1 et/ou IEC 60079-29-4).

7.2.9 Unité de commande de détection de gaz (unité logique)

Exigences:

Toutes les capacités SIL:

Une unité de commande de détection de gaz (unité logique) étant un élément de production normalisé vendu par le constructeur, les composants individuels, y compris le logiciel correspondant, doivent par conséquent être conformes aux IEC 61508-1, IEC 61508-2 et IEC 61508-3.

Une unité de commande de détection de gaz (unité logique) doit être conforme aux normes (métrologiques) de performance applicables (voir IEC 60079-29-1 et/ou IEC 60079-29-4).

7.2.10 Élément terminal (actionneur)

Exigences:

Toutes les capacités SIL:

Un élément terminal (actionneur) étant un article de production normalisé vendu par le constructeur, l'élément terminal doit être conforme aux IEC 61508-1, IEC 61508-2 et IEC 61508-3.

NOTE Si des actionneurs conformes au SIL ne sont pas disponibles, il est possible d'envisager l'utilisation des actionneurs qui sont surveillés par des composants externes de diagnostic conformes au SIL (par exemple, surveillance de la position d'une vanne à balle).

7.2.11 Indication visuelle

7.2.11.1 Caractérisation

Des panneaux indicatifs visuels sont utilisés pour afficher des informations en état normal, d'alarme ou spécial et pendant les opérations de configuration et de maintenance du système

fixe de détection de gaz. La complexité des panneaux d'indication visuelle est susceptible de varier.

Il est possible que certains systèmes fixes de détection de gaz n'utilisent pas de panneaux d'indication visuelle.

7.2.11.2 Exigences

Toutes les capacités SIL:

Toutes les indications visuelles doivent être sans ambiguïté et peuvent afficher les informations suivantes:

- les valeurs mesurées de gaz et leurs unités de mesure;
- la condition d'alarme;
- l'étendue de mesure inférieure et supérieure;
- la condition d'état spécial;
- les données de configuration;
- les données de diagnostic;
- l'état spécial ou la condition de défaut de l'équipement périphérique et/ou de l'équipement de détection de gaz associé.

Il doit être possible de régler la priorité des indications visuelles ci-dessus et ces réglages doivent être documentés.

Tous les panneaux de visualisation doivent être conformes aux normes métrologiques de performance.

Exigences supplémentaires pour les capacités SIL 2:

Un dispositif d'autotest de tous les éléments d'affichage doit être fourni sur demande de l'utilisateur. L'utilisateur doit pouvoir évaluer le résultat de l'autotest.

7.2.12 Sorties de commutation

7.2.12.1 Caractérisation

Les sorties de commutation émettent des alarmes et des signaux d'état spécial ou peuvent initier des actions de sécurité dans les équipements externes au système fixe de détection de gaz.

7.2.12.2 Exigences

Toutes les capacités SIL:

Les sorties de commutation doivent être déclenchées par les alarmes activées par le gaz et les conditions d'état spécial, qu'il s'agisse d'alarmes ou de conditions simples, groupées ou mode à vote.

Les sorties de défaut doivent être de sécurité intrinsèque.

Toutes les sorties de commutation doivent être régulièrement soumises à des essais périodiques. La fréquence des essais périodiques doit être détaillée dans le plan de maintenance.

La configuration de l'alarme activée par le gaz et les sorties de commutation de l'état spécial sont facultatives; si la configuration est de sécurité intrinsèque, il convient de prendre en compte les alarmes parasites dans une condition de défaillance de l'alimentation.

La fonction et la configuration de toutes les sorties de commutation doivent être indiquées dans la spécification des exigences de sécurité.

Toutes les alarmes doivent rester enclenchées jusqu'à leur réinitialisation manuelle, sauf indication contraire dans la spécification des exigences de sécurité.

Toutes les sorties de commutation doivent être capables de fonctionner dans leurs conditions de pleine charge, comme spécifié par le fabricant du dispositif.

NOTE Généralement, ces conditions de pleine charge seront égales à 60 % des valeurs spécifiées par le fabricant du relais pour éviter les contacts soudés.

La spécification de sécurité doit spécifier le nombre maximal de sorties de commutation au sein d'un système complet, d'un sous-système, d'un groupe de vote, ou de boucles individuelles ou groupées qui sont désactivées (neutralisées) pour des besoins de maintenance.

Exigences supplémentaires pour les capacités SIL 2:

On doit utiliser soit un relais conforme au SIL 2 en tenant compte de l'ensemble des limitations d'utilisation indiquées par le fabricant du relais, soit appliquer deux des trois options suivantes:

- a) Utilisation d'une fonction de sortie sous tension en mode de fonctionnement normal.
- b) Limitation de la charge des contacts du relais à 60 % du courant assigné spécifié dans la fiche technique du composant.
- c) Surveillance du circuit d'entrée (par exemple, bobine de relais) des sorties de commutation.

Exigences supplémentaires pour les capacités SIL 3:

Deux sorties de commutation indépendantes, chacune conforme à la capacité SIL 2, doivent être prévues pour chaque fonction de sécurité.

ou

Un relais conforme au SIL 3 doit être utilisé en tenant compte de l'ensemble des limitations d'utilisation indiquées par le fabricant du relais.

La surveillance du circuit de sortie (par exemple, en utilisant des relais à contacts de contrainte ou en évaluant un contact de report d'information) n'améliore pas la proportion de défaillances en sécurité car un éventuel défaut ne sera pas détecté tant que la fonction de sécurité n'est pas réellement requise. Des procédures opérationnelles supplémentaires sont nécessaires pour initier la fonction de sécurité si un défaut de ce type est détecté.

7.2.13 Sorties de protocole

7.2.13.1 Caractérisation

Les sorties de protocole de sécurité peuvent faire partie intégrante de la fonction de sécurité. Les sorties de protocole non relatives à la sécurité ne font pas partie de la fonction de sécurité et peuvent être utilisées à des fins de visualisation, de stockage des événements (avec avertissement sur la capacité de stockage restante), d'interrogation et autres objectifs similaires non relatifs à la sécurité uniquement.

7.2.13.2 Exigences

Les sorties de protocole de sécurité doivent se conformer à l'IEC 61508. Les sorties de protocole non relatives à la sécurité ne doivent pas être capables d'affecter de façon défavorable la fonction de sécurité du système fixe de détection de gaz.

7.2.14 Entrées de protocole

7.2.14.1 Caractérisation

Les entrées de protocole de sécurité peuvent faire partie intégrante de la fonction de sécurité. Les entrées de protocole non relatives à la sécurité ne font pas partie de la fonction de sécurité et peuvent être utilisées à des fins de visualisation, de stockage des événements (avec avertissement sur la capacité de stockage restante), d'interrogation et autres objectifs similaires non relatifs à la sécurité uniquement.

7.2.14.2 Exigences

Les entrées de protocole de sécurité doivent se conformer à l'IEC 61508. Les entrées de protocole non relatives à la sécurité ne doivent pas être capables d'affecter de façon défavorable la fonction de sécurité du système fixe de détection de gaz.

7.2.15 Architecture système, valeurs PFD et PFH

Les contraintes architecturales définies par l'IEC 61508 s'appliquent à un système fixe de détection de gaz. Chaque détecteur de gaz, sous-système et système complet doit s'y conformer.

Pour les industries de transformation, l'IEC 61511 peut être utilisée.

Les valeurs de probabilité de défaillance en cas de sollicitation (PFD – probability of failure on demand) définies par l'IEC 61508 s'appliquent à un système fixe de détection de gaz. La somme totale de toutes les valeurs de PFD pour les sous-systèmes, utilisées dans une seule boucle de sécurité de détection de gaz, doit être conforme à l'objectif d'intégrité de sécurité défini dans la spécification de sécurité.

Pour les applications nécessitant un mode à forte sollicitation ou continu, les valeurs de probabilité de défaillance en cas de forte sollicitation (PFH) doivent être spécifiées conformément à l'IEC 61508.

8 Exigences uniques de détection de gaz

8.1 Objectifs

L'objectif premier du présent article est de définir comment satisfaire aux exigences uniques d'un système fixe de détection de gaz utilisé en tant que système instrumenté de sécurité.

Le second objectif du présent article est de définir comment il convient que l'équipement associé de détection de gaz, qui fait partie de la fonction de sécurité et contribue au fonctionnement du système fixe de détection de gaz, se conforme à la présente Norme internationale. L'équipement associé de détection de gaz comporte:

- des échantillonneurs de gaz;
- des multiplexeurs de gaz;
- des unités de commande du multiplexeur de gaz;
- des dispositifs de conditionnement de gaz;
- des unités d'étalonnage et d'ajustement automatiques de gaz.

Si une unité fonctionnelle n'est pas décrite dans l'Article 8, il convient alors de suivre la procédure de l'Annexe C afin de vérifier la capacité SIL pour cette unité fonctionnelle.

8.2 Exigences

8.2.1 Introduction à l'échantillonnage de gaz

Dans un système à aspiration, la ou les pompes, la surveillance des flux et le conditionnement final de l'échantillon, ainsi que toutes les caractéristiques associées au multiplexage, font généralement partie intégrante d'un système manufacturé, qui peut aussi inclure des composants de conditionnement de point d'échantillonnage. Cependant, l'intégrité globale est influencée dans une grande mesure par la sélection, l'installation et la maintenance d'éléments du système d'échantillonnage du gaz, en particulier les tubes d'échantillonnage installés et l'emplacement de l'équipement de point d'échantillonnage. Pour ce qui concerne les exigences et les recommandations relatives à ces aspects, il convient de se reporter à l'IEC 60079-29-2. Dans ce domaine, la conception constitue une tâche hautement spécialisée qui nécessite de plus d'être conforme à l'IEC 61508.

8.2.2 Échantillonnage du gaz

8.2.2.1 Caractérisation

L'aspiration de gaz est assurée par les éléments suivants: ligne d'échantillonnage, pompe d'aspiration de gaz, réglage du débit d'échantillonnage (vanne de dérivation ou de réduction), aspiration de gaz vers le capteur et surveillance du débit.

8.2.2.2 Exigences

Toutes les capacités SIL:

L'aspiration de gaz doit être conçue de sorte qu'une perte de continuité ou une restriction de l'aspiration de gaz doit être détectée. La pénétration d'air ou la perte de gaz à mesurer due à une fuite doit être empêchée ou doit être détectée et signalée.

L'inspection de la totalité des points d'échantillonnage, des lignes d'échantillonnage, des pompes, des filtres, etc., doit être effectuée fréquemment. La fréquence de l'inspection est déterminée par l'application, l'intégrité SIL et les conditions environnementales.

Capacités SIL 1 et 2:

Les variations de débit du gaz doivent être surveillées près du capteur (limite inférieure ou supérieure si nécessaire). Les conditions de débit qui ne satisfont pas aux exigences fonctionnelles, par exemple pour la réponse, doivent être détectées. Deux dispositifs de surveillance au minimum doivent être fournis. Il peut s'agir de contrôleurs de débit ou de pression/vide; ils doivent être placés avec la plus grande attention. Si le multiplexage d'échantillonnage (voir multiplexeur de gaz) est utilisé, il convient de placer ces dispositifs de surveillance entre les vannes de multiplexage et le capteur de façon à détecter aussi toute défaillance dans le module de multiplexage provoquant des erreurs de distribution d'échantillon.

Des éléments de diagnostic avec leurs taux de défaillance doivent être appliqués à l'analyse AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité), mais n'ont pas à se conformer au SIL lui-même.

Exigences supplémentaires pour les capacités SIL 3:

Un montage protégé et ajusté des lignes d'échantillonnage jusqu'au capteur doit être assuré conjointement à la surveillance du débit, comme spécifié pour la capacité SIL 1 et 2.

"Protégé" signifie une installation dans laquelle il est peu probable qu'une fuite d'origine mécanique puisse se produire, par exemple les lignes d'échantillonnage peuvent être en acier inoxydable ou autre matériau compatible avec l'échantillon. Il convient d'éviter les lignes flexibles ou de les protéger en les installant dans une conduite ou une canalisation supplémentaire ou dans un boîtier fermé en fonctionnement normal.

"Ajusté" signifie l'utilisation de connexions soudées ou de raccords pour tube à compression.

Des éléments de diagnostic avec leurs taux de défaillance doivent être appliqués à l'analyse AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité) mais n'ont pas à se conformer au SIL lui-même.

8.2.3 Multiplexeur de gaz

8.2.3.1 Caractérisation

Le multiplexeur de gaz comprend une sélection de lignes d'échantillonnage et peut comporter la purge ou la dérivation des lignes d'échantillonnage.

Les points d'échantillonnage individuels sont sélectionnés de façon séquentielle. L'échantillon de gaz prélevé au point de mesure sélectionné traverse le multiplexeur de gaz et est mesuré au niveau du capteur.

La purge de la ligne d'échantillonnage est un processus au cours duquel un échantillon de gaz frais est prélevé pour remplir la ligne d'échantillonnage avant de sélectionner la ligne de ce point d'échantillonnage. Cela peut être réalisé au moyen d'une pompe de dérivation prélevant un échantillon sur la ligne à échantillonner suivante ou bien en prélevant à tout moment sur toutes les lignes qui ne sont pas échantillonnées. Cela réduit le temps nécessaire à chaque mesure individuelle.

Le multiplexeur de gaz implique l'existence de la commande de l'échantillonnage de gaz et du multiplexeur de gaz.

8.2.3.2 Exigences

Toutes les capacités SIL:

A chaque ligne d'échantillonnage, le flux de gaz doit être surveillé près du capteur et près du point d'échantillonnage (limite inférieure ou supérieure si nécessaire). Les conditions de débit qui ne satisfont pas aux exigences fonctionnelles, par exemple pour le temps de réponse, doivent être détectées et indiquées par un signal transmissible.

Le principe d'échantillonnage du gaz doit être appliqué pour la protection contre la pénétration d'air et le blocage. Outre la protection contre la dilution des échantillons par des blocages et des fuites, des précautions doivent aussi être prises pour s'assurer que l'échantillon présenté au capteur n'est pas contaminé par l'échantillon provenant d'un autre flux.

Exigences supplémentaires pour la capacité SIL 2:

Les signaux de surveillance des flux de tous les points de mesure doivent être traités (dans un module de commande du multiplexeur de gaz) de manière continue. Un flux ne doit être détecté qu'au niveau des lignes effectivement échantillonnées ou purgées. Une seule limite de seuil est suffisante pour faire la distinction entre "débit" et "pas de débit".

Exigences supplémentaires pour la capacité SIL 3:

Pour faire la distinction entre "flux" et "pas de flux", il doit y avoir deux limites de seuil séparées (près de zéro et près du point de consigne). Un faible flux doit être détecté dans la ligne d'échantillonnage et le flux de fuite doit être détecté dans les lignes d'échantillonnage qui ne sont pas utilisées.

L'inspection de la totalité des points d'échantillonnage, des lignes d'échantillonnage, des pompes, des filtres, des vannes, etc., doit être effectuée fréquemment. La fréquence de l'inspection est déterminée par l'application, la capacité SIL et les conditions environnementales.

8.2.4 Système de commande du multiplexeur de gaz

8.2.4.1 Caractérisation

Le système de commande du multiplexeur de gaz sélectionne les points de mesure à partir desquels le gaz est envoyé au capteur. Il garantit que le calcul et l'évaluation des valeurs de mesure sont associés au point de mesure correct. Il démarre également une action de déclenchement d'alarme au système fixe de détection de gaz lorsqu'un état spécial ou une condition de défaut se déclare au sein de l'échantillonneur de gaz, du multiplexeur de gaz ou du système de commande du multiplexeur de gaz.

Dans le cas le plus simple, les points de mesure peuvent être sélectionnés de façon cyclique. Cependant, il est possible que des séquences plus complexes soient requises, par exemple des séquences déclenchées par les événements.

8.2.4.2 Exigences

Toutes les capacités SIL:

Le système de commande du multiplexeur de gaz doit surveiller que le traitement se déroule correctement en évaluant les indications d'état au sein du système de commande du multiplexeur de gaz. Si les indications d'état ne sont pas correctes, le système doit signaler un défaut.

Si la commutation est déclenchée par les événements, la prolongation du temps de cycle maximal pour les points de mesure non activés doit être comprise dans un intervalle de temps spécifié, dépendant de l'application. Si le temps de cycle dépasse cet intervalle, le système doit signaler un défaut.

Le système de commande du multiplexeur de gaz, qui comprend des capteurs de débit/pression, des dispositifs de traitement logique, d'alarme et de transition vers une logique d'état spécial, définit une fonction de sécurité de sous-système qui doit elle-même démontrer qu'elle atteint la capacité SIL maximale de la fonction de sécurité à laquelle appartient le module de multiplexeur de gaz.

8.2.5 Conditionnement du gaz mesuré

8.2.5.1 Caractérisation

Le conditionnement de l'échantillon de gaz aspiré peut comprendre un ou plusieurs éléments, notamment une sonde, un filtre, un convertisseur chimique, un appareil de chauffage de la ligne d'échantillonnage, un refroidisseur de gaz, un piège à eau et un déshumidificateur.

8.2.5.2 Exigences

Le conditionnement du gaz mesuré implique l'existence de l'échantillonneur de gaz et l'application des exigences spécifiées dans l'article relatif à l'échantillonnage de gaz.

Toutes les capacités SIL:

Les instructions données dans le manuel de sécurité doivent permettre à l'utilisateur de calculer le temps de fonctionnement admissible pour les éléments disposant d'un temps de fonctionnement limité (par exemple des filtres qui peuvent saturer). Ces éléments doivent être remplacés avant d'avoir atteint la limite de leur temps de fonctionnement. Les exigences de performance applicables au système de conditionnement exigé pour l'application doivent être spécifiées dans le manuel de sécurité de l'unité fonctionnelle ou du système de détection de gaz, par exemple, la plage de température admissible si un appareil de chauffage ou de refroidissement est exigé.

Exigences supplémentaires pour les capacités SIL 2:

La fonction de tout élément unique nécessaire à la sécurité fonctionnelle doit être:

- soumise à un régime d'inspections régulières sur la base des recommandations du constructeur et compte tenu des conditions du site; ou
- accompagnée de diagnostics ou de surveillance en ligne appropriés pour en garantir le bon fonctionnement (par exemple, surveillance de la température maximale d'un refroidisseur électrique de gaz). Des éléments de diagnostic avec leurs taux de défaillance doivent être appliqués à l'analyse AMDEC mais n'ont pas à se conformer au SIL lui-même.

Exigences supplémentaires pour les capacités SIL 3:

Des diagnostics ou une surveillance en ligne appropriés doivent être prévus pour garantir le bon fonctionnement (par exemple, la surveillance de la plage de température d'un refroidisseur électrique de gaz).

En règle générale, il n'est pas possible d'obtenir le SIL 3 au moyen d'une seule chaîne et il est généralement nécessaire de dupliquer toute la chaîne de mesure, de l'entrée du gaz à l'élément sensible. Des éléments de diagnostic avec leurs taux de défaillance doivent être appliqués à l'analyse AMDEC mais ils n'ont pas à se conformer au SIL lui-même.

8.2.6 Échantillonnage de gaz en mode diffusion

8.2.6.1 Caractérisation

L'échantillonnage de gaz est basé sur des éléments tels que des filtres ou des convertisseurs chimiques; par exemple, les filtres comportent des disques métalliques frittés, des barrières hydrophobes, des disques de papier, etc. La plupart des filtres et des convertisseurs chimiques peuvent disposer d'un temps de fonctionnement limité du fait de leur saturation ou altération.

8.2.6.2 Exigences

Toutes les capacités SIL:

Les instructions données dans le manuel de sécurité doivent permettre à l'utilisateur de calculer le temps de fonctionnement des éléments disposant d'un temps de fonctionnement limité (par exemple, saturation des filtres à cause de la poussière). Ces éléments doivent être remplacés ou nettoyés avant d'avoir atteint la limite de leur temps de fonctionnement, sur la base des recommandations du constructeur et compte tenu des conditions du site.

Lorsqu'un type quelconque de filtre ou de disque métallique fritté comprend un écran de diffusion, l'installation doit garantir que de l'eau ou un autre liquide ne peut entrer en contact avec le filtre ou le disque et le bloquer, tout en permettant le libre accès du gaz et de la vapeur. Si le constructeur dispose d'un accessoire normalisé à cet effet, ses limites doivent être spécifiées.

Exigences supplémentaires pour les capacités SIL 2:

La fonction de tous les composants nécessaires à la sécurité fonctionnelle doit être régulièrement inspectée ou confirmée par des essais de diagnostic en ligne (par exemple un étalonnage automatique).

Exigences supplémentaires pour les capacités SIL 3:

Ceci n'est pas réalisable dans le cas d'unités fonctionnelles uniques, à moins de pouvoir démontrer que les défauts qui empêchent le gaz prélevé d'atteindre le capteur ne sont pas crédibles. Dans ce cas, aucune exigence supplémentaire ne s'applique à la capacité SIL 2.

8.2.7 Étalonnage et ajustement automatiques

8.2.7.1 Caractérisation

L'étalonnage automatique de l'unité fonctionnelle est assuré par les éléments suivants: moyens d'étalonnage (par exemple, bouteille de gaz, générateur de gaz, cellule à gaz de référence), conduite de gaz d'essai, pompe d'aspiration de gaz, réglage du débit d'échantillonnage (dérivation ou vannes), aspiration du gaz vers le capteur (masque d'étalonnage ou cellule à circulation) et surveillance du débit.

L'étalonnage automatique de l'unité fonctionnelle implique l'existence du système de commande de l'étalonnage automatique de l'unité fonctionnelle.

L'étalonnage automatique peut ou non inclure un ajustement automatique.

8.2.7.2 Exigences

Toutes les capacités SIL:

Pour éviter les déclenchements parasites, une condition d'état spécial doit être activée avant le lancement de l'étalonnage automatique. Un contrôle de vraisemblance doit être effectué au cours de l'application du gaz d'essai, par exemple, en définissant une tolérance pour la sensibilité/l'étalonnage existants. La condition d'état spécial doit être désactivée immédiatement après la réussite de l'étalonnage. Si l'étalonnage échoue, l'état spécial doit être automatiquement désactivé après une période définie, les données antérieures d'étalonnage doivent être conservées et un défaut doit être signalé. Toutes ces fonctions doivent être mises en œuvre dans l'unité fonctionnelle "commande de l'étalonnage automatique" ou dans le système "fixe de détection de gaz".

Un étalonnage est réussi si:

- les débits pendant l'étalonnage se situent dans les limites acceptables;
- la vitesse de la réponse avec application du gaz zéro ou du gaz d'étalonnage se situe dans un ensemble défini de limites;
- les valeurs finales d'étalonnage respectent une tolérance spécifiée ou un ajustement automatique est réalisé;
- les valeurs finales d'étalonnage après ajustement respectent une tolérance spécifiée des valeurs, immédiatement avant ajustement (par exemple, une dérive excessive entre des étalonnages successifs); et
- les valeurs finales d'étalonnage ne dépassent pas les limites d'ajustement recommandées par le constructeur (par exemple, un ajustement cumulativement excessif).

En plus des points précédents, des précautions contre la contamination croisée des gaz d'étalonnage doivent être prises selon la même méthode de base que pour le multiplexage de gaz.

Tous les événements d'étalonnage automatique doivent être automatiquement enregistrés par l'unité fonctionnelle "commande de l'étalonnage automatique" ou par le système "fixe de détection de gaz".

L'étalonnage automatique ne remplace pas la nécessité d'une inspection manuelle du système fixe de détection de gaz. L'inspection manuelle planifiée doit être réalisée selon le plan de maintenance.

8.2.8 Système de commande de l'étalonnage et de l'ajustement automatiques

8.2.8.1 Caractérisation

Le système de commande de l'étalonnage automatique sélectionne le capteur pour lequel la procédure d'étalonnage est à exécuter. Cela garantit que l'état spécial "étalonnage" est établi, surveillé et quitté à la fin du processus d'étalonnage.

L'initiation de la procédure d'étalonnage peut être effectuée automatiquement selon un programme défini dans l'unité de commande (par exemple, à une fréquence temporelle définie) sur demande de l'utilisateur ou sur demande du système fixe de détection de gaz.

8.2.8.2 Exigences

Toutes les capacités SIL:

L'étalonnage automatique ne doit être déclenché que pour les points de mesure qui sont en mode mesure et ne sont pas en condition d'alarme.

Outre la sélection du point de mesure, l'unité de commande doit surveiller le déroulement et l'évaluation corrects de la procédure d'étalonnage. Cela doit garantir que l'état spécial "étalonnage" est établi, surveillé et quitté à la fin du processus. Les données d'étalonnage existantes (paramètres) ne doivent être remplacées qu'après réussite de l'étalonnage.

Tous les résultats d'étalonnage doivent être automatiquement enregistrés, y compris l'intervalle entre les étalonnages et l'heure et la date de l'étalonnage.

Les procédures opérationnelles supplémentaires doivent être en place pour assurer que les gaz d'étalonnage utilisés au cours du processus d'étalonnage automatique:

- n'ont pas dépassé leur date d'expiration;
- sont des mélanges certifiés de gaz, y compris la teneur en oxygène si nécessaire.

NOTE Généralement, une concentration de gaz d'essai d'étalonnage à 50% au milieu de l'étendue est appliquée.

9 Unités de commande alternatives (unités logiques)

9.1 Objectifs

L'objectif de l'Article 9 est de définir comment les unités de commande alternatives (unités logiques) à l'unité de commande dédiée du constructeur peuvent être utilisées dans l'ensemble d'un système fixe de détection de gaz ou un sous-système.

9.2 Exigences

9.2.1 Performances (métrologiques)

Toute unité de commande alternative (unité logique) doit démontrer au moins sa conformité aux exigences métrologiques de performance pour les systèmes fixes de détection de gaz et doit disposer de la capacité SIL.

9.2.2 Programmation logique

La programmation logique de l'unité de commande alternative (unité logique) doit garantir que tous les états spéciaux et les alarmes de défaut observés dans les systèmes fixes de détection de gaz sont traités conformément à la présente Norme internationale et aux normes métrologiques de performance pertinentes (voir l'IEC 60079-29-1 et l'IEC 60079-29-4).

NOTE Pour des lignes directrices sur la programmation de l'unité logique, voir l'IEC 61511.

Une attention particulière doit être portée à la compétence des individus lorsque des unités logiques alternatives sont utilisées dans une application d'un système fixe de détection de gaz (voir Article 7).

10 Essais de réception en usine

10.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales, notamment la documentation nécessaire, qu'il convient d'appliquer lors de la phase des essais de recette en usine.

10.2 Exigences

10.2.1 Planification

Il convient de spécifier la nécessité d'un essai de recette en usine au cours de la phase de conception et d'ingénierie ou dans l'étendue de la fourniture. Il convient d'indiquer au minimum les points suivants:

- les types d'essais à effectuer;
- les critères D'ACCEPTATION/DE REFUS, notamment le moment auquel interrompre les essais sujets à des défaillances simples ou multiples;
- les procédures d'enregistrement des données/résultats des essais et les versions matérielle/logicielle de l'équipement soumis à l'essai;
- les procédures relatives aux actions correctives;
- les procédures relatives aux modifications ou changements apportés au système;
- les procédures relatives à la gestion des conflits;
- les exigences minimales de configuration du système;
- les dépendances à l'égard des équipements ou interfaces tiers;
- les équipements d'essai à utiliser, étayés par des certificats valides d'étalonnage des équipements;
- les gaz d'essai à utiliser, étayés par des certificats valides de composition de gaz;
- les compétences des personnes chargées de l'essai et des personnes présentes;
- l'emplacement de la zone protégée, tout gaz toxique ou inflammable spécial et les précautions correspondantes prises;
- une description de tout essai "boîte noire"; et
- les exclusions.

NOTE Les essais de réception en usine s'appliquent normalement aux sous-systèmes et aux systèmes mais pas aux détecteurs de gaz autonomes, sauf spécification particulière dans le contrat d'approvisionnement d'équipement.

Lorsque la totalité du système est sous la responsabilité d'un intégrateur système, la planification de l'essai de recette en usine est sous la responsabilité de l'intégrateur système, sauf spécification contraire.

10.2.2 Réalisation

Il convient de réaliser les essais de réception en usine conformément au plan d'essai de réception en usine.

Avant la réalisation des essais de réception en usine, les vérifications suivantes doivent être effectuées pour toute la documentation:

- exhaustivité de la documentation;
- révision correcte;
- au minimum, approbation pour construction système (AFC – approved for system construction), pour tous les documents.

Si une défaillance se produit pendant les essais de réception en usine, il convient d'identifier et de documenter la raison de cette défaillance. Il convient de choisir entre les options suivantes:

- réparer la défaillance et soumettre à nouveau à l'essai;
- ignorer la défaillance et terminer l'essai du système;
- arrêter tout le programme d'essai si la défaillance affecte l'ensemble du système, ce qui permet de réparer la défaillance, et choisir une nouvelle date pour l'essai; ou
- terminer partiellement les essais et programmer un essai partiel supplémentaire de réception en usine.

Si, au cours des essais de réception en usine, le système subit des modifications ou des changements, il convient de les soumettre à une analyse de sécurité pour déterminer:

- l'ampleur de l'impact sur chaque fonction de sécurité; et
- l'ampleur des éventuels nouveaux essais qu'il convient de définir et de réaliser.

11 Installation et mise en service

11.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales, notamment la documentation nécessaire, qu'il convient d'appliquer lors de la phase d'installation et de mise en service.

11.2 Exigences

11.2.1 Planification

Il convient de spécifier les méthodes d'installation et les procédures de mise en service au cours de la phase de conception du système fixe de détection de gaz. Il convient qu'elles comprennent au moins les points suivants:

- les activités d'installation;
- les éventuelles précautions particulières exigées pour l'installation (recommandations des fournisseurs du dispositif);
- la personne, le service ou l'organisation responsable des activités d'installation;
- les précautions à prendre lorsque l'installation est située dans une zone dangereuse;
- les essais électriques exigés pour vérifier que l'installation électrique est correcte (avant la mise sous tension du système);
- les types d'essais à effectuer lors du démarrage du système;
- les critères D'ACCEPTATION/DE REFUS, notamment le moment auquel interrompre les essais sujets à des défaillances simples ou multiples;

- les procédures d'enregistrement des données/résultats des essais et les versions matérielle/logicielle de l'équipement en essai;
- les procédures relatives aux actions correctives;
- les procédures relatives aux modifications ou aux changements apportés au système;
- les procédures relatives à la gestion des conflits;
- les équipements d'essai à utiliser, étayés par des certificats valides d'étalonnage des équipements;
- les gaz d'essai à utiliser, étayés par des certificats valides de composition des gaz;
- les compétences des personnes chargées de l'essai et des personnes présentes;
- les précautions prises pour tout gaz toxique ou inflammable spécial; et
- les exclusions.

11.2.2 Réalisation

Il convient de réaliser l'installation conformément au plan d'installation.

Il convient de réaliser la mise en service conformément au plan de mise en service.

Avant l'installation et la mise en service, les vérifications suivantes doivent être effectuées pour toute la documentation:

- exhaustivité de la documentation;
- révision correcte;
- approbation pour l'installation et la mise en service du système.

Si une défaillance se produit pendant la mise en service, il convient d'identifier et de documenter la raison de cette défaillance. Il convient de choisir entre les options suivantes:

- réparer la défaillance et poursuivre l'opération de mise en service;
- ignorer la défaillance et terminer l'opération de mise en service;
- arrêter toute l'opération de mise en service si la défaillance affecte l'ensemble du système, ce qui permet de réparer la défaillance, et choisir une nouvelle date pour l'essai; ou
- terminer partiellement l'opération de mise en service et programmer une activité de mise en service finale supplémentaire.

Si, au cours de l'opération de mise en service, le système subit des modifications ou des changements, il convient de les soumettre à une analyse de sécurité pour déterminer:

- l'ampleur de l'impact sur chaque fonction de sécurité; et
- l'ampleur des éventuels nouveaux essais qu'il convient de définir et de réaliser.

Toutes les modifications doivent être documentées.

12 Validation du système¹

12.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales, notamment la documentation nécessaire, qu'il convient d'appliquer lors de la phase de validation du système.

1 Généralement appelée essai de réception sur site (SAT – Site Acceptance Test)

NOTE La validation du système prend en compte l'ensemble du système et l'intégration correcte des composants des différents constructeurs.

12.2 Exigences

12.2.1 Planification

Il convient de spécifier la nécessité d'un essai de validation du système au cours de la phase de conception du système fixe de détection de gaz. Il convient qu'il comprenne au moins les points suivants:

- des méthodes de validation pour garantir que le système fixe de détection de gaz installé remplit la fonction de sécurité comme indiqué dans la spécification des exigences de sécurité;
- des méthodes de validation pour garantir que le système fixe de détection de gaz installé fonctionne correctement:
 - en fonctionnement normal;
 - en fonctionnement anormal (mauvaise utilisation);
 - en condition d'état spécial; et
 - en condition de défaut;
- une méthode permettant d'inclure toute modification du système qui peut avoir été mise en œuvre au cours des essais de réception en usine, de l'installation du système ou de la mise en service du système;
- la validation des compétences des personnes et des personnes présentes; et
- les procédures d'enregistrement des données/résultats des essais et les versions matérielle/logicielle de l'équipement en essai.

12.2.2 Réalisation

Il convient de réaliser les essais de validation du système conformément au plan d'essai de validation du système.

Avant la réalisation des essais de validation du système, les vérifications suivantes doivent être effectuées pour toute la documentation:

- exhaustivité de la documentation;
- révision correcte; et
- au minimum, approbation pour construction et installation système (AFCI – approved for system construction and installation), pour tous les documents.

Si une défaillance se produit pendant les essais de validation du système, la raison de cette défaillance doit être identifiée et documentée. Un choix doit être fait entre les options suivantes:

- réparer la défaillance et revalider;
- ignorer la défaillance et terminer la validation du système;
- arrêter tout le programme de validation si la défaillance affecte l'ensemble du système, ce qui permet de réparer la défaillance, et choisir une nouvelle date pour la validation; ou
- terminer partiellement la validation et programmer un essai partiel supplémentaire de validation du système.

Si, au cours des essais de validation du système, le système subit des modifications ou des changements, il convient de les soumettre à une analyse de sécurité pour déterminer:

- l'ampleur de l'impact sur chaque fonction de sécurité; et
- l'ampleur des nouveaux essais qu'il convient de définir et de réaliser.

Tant que toutes les exigences détaillées dans l'essai de validation du système ne sont pas validées par rapport à la spécification des exigences de sécurité, le système fixe de détection de gaz ne peut être considéré comme étant opérationnel.

13 Exploitation et maintenance

13.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales, y compris les exigences de service individuelles nécessaires, notamment les essais périodiques, qu'il convient d'appliquer lors de la phase d'exploitation et de maintenance.

13.2 Exigences

13.2.1 Planification

Il convient de spécifier la nécessité de la planification de l'exploitation et de la maintenance au cours de la phase de conception du système fixe de détection de gaz. Il convient qu'elle comprenne au moins les points suivants:

- des enregistrements détaillés des performances du système en fonctionnement normal, y compris en état spécial et en conditions de défaut;
- le nombre de sollicitations du système;
- toute mauvaise utilisation ou tout fonctionnement anormal du système;
- les données environnementales applicables associées à chaque point de mesure;
- la fréquence des activités planifiées de maintenance du système;
- le nombre maximal de boucles de sécurité neutralisées pendant les activités de maintenance;
- les mesures opérationnelles supplémentaires à prendre pendant les activités de maintenance;
- les enregistrements détaillés de maintenance, notamment les défauts relevés, les actions de correction ou de réparation entreprises, les pièces de rechange et les consommables utilisés et les modifications des performances du système susceptibles d'affecter à l'avenir la fonction de sécurité;
- les résultats détaillés des essais périodiques; et
- le détail des actions correctives entreprises si un essai périodique échoue.

13.2.2 Réalisation

Le système fixe de détection de gaz doit fonctionner comme détaillé dans le manuel de sécurité de l'ensemble du système et dans les manuels pertinents d'utilisation des équipements individuels.

Les individus en charge des activités d'exploitation, d'intervention ou de maintenance du système fixe de détection de gaz doivent être compétents en la matière et disposer des autorisations correspondantes.

NOTE 1 Pour de plus amples informations sur la compétence, voir 6.3.

Le système fixe de détection de gaz doit être maintenu comme détaillé dans le plan de maintenance de l'ensemble du système. Seuls les pièces de rechange et les consommables énumérés dans le manuel de sécurité ou les manuels de maintenance des équipements individuels doivent être utilisés.

Le système fixe de détection de gaz doit être soumis aux essais périodiques comme détaillé dans le manuel de sécurité du système.

L'efficacité de l'essai périodique dépend de la mesure dans laquelle le système a été rétabli dans la condition "comme neuf". Pour que l'essai périodique soit pleinement efficace, il est nécessaire de détecter 100 % des défaillances dangereuses. Bien que dans la pratique, il ne soit pas facile de détecter 100 % des défaillances dangereuses pour des systèmes autres que les systèmes E/E/PE relatifs à la sécurité de faible complexité, il convient de conserver cet objectif. Au minimum, toutes les fonctions de sécurité qui sont exécutées sont contrôlées selon la spécification des exigences de sécurité des systèmes E/E/PE. Si des canaux séparés sont utilisés, ces essais sont effectués séparément pour chacun des canaux.

Toutes les activités doivent être clairement documentées.

14 Modification du système

14.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales, notamment la documentation nécessaire, qu'il convient d'appliquer lors de la phase de modification du système.

14.2 Exigences

14.2.1 Planification

Avant d'être effectuée, toute modification apportée à tout système fixe de détection de gaz doit être planifiée, revue et autorisée. Le plan doit présenter un niveau acceptable de sécurité pendant et après la modification.

La planification doit comporter:

- une analyse d'impact;
- la continuité de la fonction de sécurité du système fixe de détection de gaz et de l'intégrité de sécurité au cours du processus de modification;
- les mesures alternatives exigées pour garantir que le niveau d'intégrité de sécurité est maintenu;
- les contraintes associées aux zones dangereuses (documentation de protection contre l'explosion);
- les méthodes de validation pour garantir que la modification a été correctement effectuée et qu'aucune des fonctions associées (non modifiées) n'a été affectée;
- les plans d'urgence si une modification n'est pas effectuée dans les temps ou si la modification ne peut être terminée ou si un événement inévitable se produit;
- des descriptions détaillées des compétences des individus qui effectuent la modification;
- le processus de contrôle de la documentation; et
- la formation du personnel une fois la modification terminée, notamment les programmes de service, l'inventaire des pièces de rechange et les procédures opérationnelles.

14.2.2 Réalisation

Une activité de modification ne doit pas commencer sans autorisation valide.

Toutes les modifications doivent être documentées, vérifiées et validées et suivre le plan, les documents et les instructions de modification.

Tout écart par rapport au plan de modification doit être autorisé et si nécessaire, il convient d'effectuer une nouvelle analyse d'impact. Si l'analyse d'impact révèle des risques inacceptables, il convient d'arrêter la modification et il faut suivre le plan d'urgence.

Lorsque la modification est terminée, tout le système ou toute la partie du système doit être validé afin de démontrer l'aptitude de la fonction de sécurité.

15 Déclassement / mise hors service du système

15.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales, notamment la documentation nécessaire, qu'il convient d'appliquer lors de la phase de déclassement du système.

15.2 Exigences

15.2.1 Planification

Avant d'être effectué, le déclassement total ou partiel d'un système fixe de détection de gaz doit être planifié, revu et autorisé. Le plan doit présenter un niveau acceptable de sécurité pendant et après le déclassement partiel ou total.

La planification doit comporter:

- une analyse d'impact;
- si nécessaire, le moyen d'assurer la continuité de la ou des fonctions de sécurité du système fixe de détection de gaz et de l'intégrité de sécurité au cours du processus de déclassement;
- les mesures alternatives exigées pour garantir que le niveau d'intégrité de sécurité est maintenu au cours du processus de déclassement;
- les contraintes associées aux zones dangereuses;
- la validation du système restant si une partie du système d'origine est à déclasser;
- les plans d'urgence si le déclassement n'est pas effectué dans les temps ou si le déclassement ne peut être terminé ou si un événement inévitable se produit;
- des descriptions détaillées des compétences des individus qui effectuent le déclassement;
- le processus de contrôle de la documentation; et
- la formation du personnel après que le déclassement est terminé, y compris les modifications des procédures opérationnelles.

15.2.2 Réalisation

Une activité de déclassement ne doit pas commencer sans autorisation valide.

Toutes les phases du plan de déclassement doivent être documentées au fur et à mesure, vérifiées et validées et suivre le plan de déclassement.

Tout écart par rapport au plan de déclassement doit être autorisé et si nécessaire, il convient d'effectuer une nouvelle analyse d'impact. Si l'analyse d'impact révèle des risques inacceptables, il convient d'arrêter le déclassement et le plan d'urgence doit être suivi.

Lorsque l'activité de déclassement est terminée, tout le système ou toute la partie du système qui a été déclassé doit être correctement éliminé.

Après l'activité de déclassement, il convient de reformer tout le personnel concerné.

16 Documentation

16.1 Objectifs

L'objectif du présent article est de souligner les exigences minimales pour toute la documentation de support nécessaire, quelle que soit la phase du cycle de vie.

16.2 Exigences

Il convient que tous les documents simples, notamment les manuels d'utilisation des instruments individuels, les manuels de sécurité, les schémas électriques, les listes des pièces de rechange, les fiches techniques, etc., soient:

- adaptés à l'objectif et applicables à l'application;
- précis et faciles à comprendre; et
- contrôlés par révision.

NOTE Il faut souvent fournir les documents aux intégrateurs systèmes.

Il convient également que tous les dossiers de documentation fournis pour étayer l'ensemble d'un système fixe de détection de gaz:

- soient indexés et contrôlés par révision;
- soient structurés de façon à rendre les informations facilement accessibles;
- comprennent des informations pertinentes pour chaque partie du cycle de vie;
- comprennent tous les résultats des essais de réception en usine (FAT), du déclassement et de la validation sur site (SAT);
- comprennent les activités de maintenance recommandées, accompagnées d'un programme d'essai de support et de fiches de suivi;
- comprennent les activités recommandées d'essai périodique, accompagnées d'un programme d'essai de support et de fiches de suivi; et
- énumèrent les pièces de rechange opérationnelles recommandées.

Il convient de constituer un manuel de sécurité complet avec au moins les informations suivantes:

- la fonction de sécurité et l'intégrité par boucle de sécurité;
- les restrictions d'utilisation, notamment des consommables, par exemple les filtres;
- les procédures opérationnelles;
- les procédures de maintenance;
- un guide de détection des défauts; et
- les procédures de neutralisation.

Il convient de fournir tous les certificats de produit accompagnés du rapport d'essai associé lorsqu'il est disponible.

Il convient que le contrôle de révision de tous les documents indique clairement le produit ou le système auquel il s'applique, ainsi que la révision matérielle et la version logicielle du produit ou du système.

Annexe A (informative)

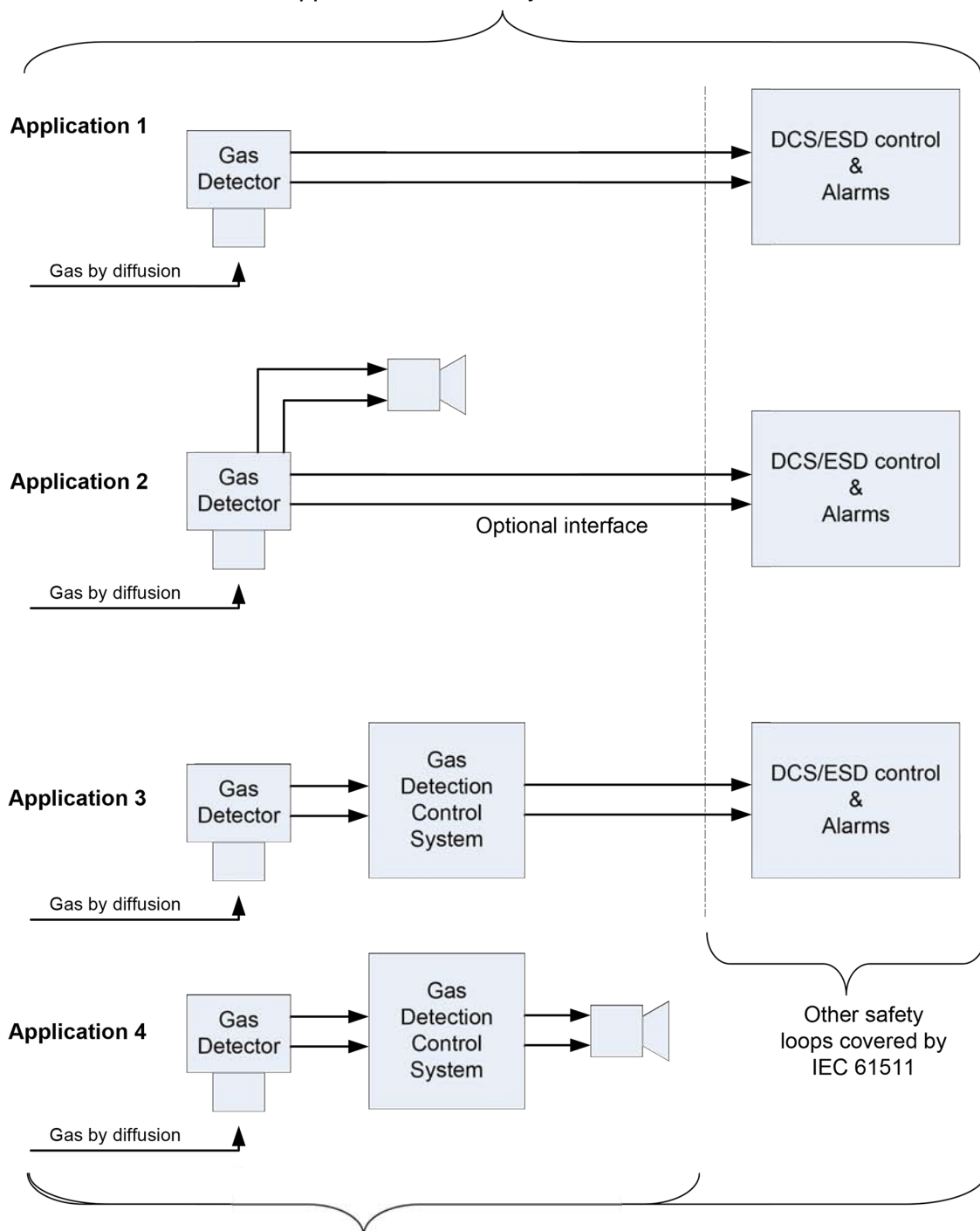
Applications typiques

A.1 Applications typiques de diffusion

A.1.1 Application 1

Gas Detection Safety Loops

Products covered by IEC 61508
Application covered by IEC 60079-29-3



Performance to IEC 60079-29-1, IEC 60079-29-4
or other performance standards for Toxic and/or Oxygen detection

Légende

Anglais	Français
Gas Detection Safety Loops	Boucles de sécurité de détection de gaz
Products covered by IEC 61508 Application covered by IEC 60079-29-3	Produits couverts par l'IEC 61508 Application couverte par l'IEC 60079-29-3
Gas Detector	Détecteur de gaz
Gas by diffusion	Gaz par diffusion
DCS/ESD control & Alarms	Contrôle DCS/ESD & alarmes
Optional interface	Interface optionnelle
Gas Detection Control System	Système de commande de détection de gaz
Other safety loops covered by IEC 61511	Autres boucles de sécurité couvertes par l'IEC 61511
Performance to IEC 60079-29-1, IEC 60079-29-4 or other performance standards for Toxic and/or Oxygen detection	Performances conformément à l'IEC 60079-29-1, à l'IEC 60079-29-4 ou à d'autres normes de performance relatives à la détection de gaz toxique et/ou d'oxygène

Figure A.1 – Boucles de sécurité de détection de gaz

Cette application couvre uniquement l'utilisation d'un détecteur fixe de gaz qui est généralement intégré à un système de commande réparti (DCS – Distributed Control System) ou à un système de commande d'arrêt d'urgence (ESD – Emergency Shut-down) (voir la Figure A.1). Le système de commande DCS ou ESD réalise la logique du système et lance l'action de sécurité.

Le détecteur de gaz correspondant à cette application est conçu et fabriqué conformément à la série IEC 61508. La fourniture, l'application, l'intégration et le fonctionnement de cette application sont couverts par la présente Norme.

A.1.2 Application 2

Cette application couvre uniquement l'utilisation d'un détecteur fixe de gaz qui réalise la logique du système et lance l'action de sécurité (voir la Figure A.1).

Le détecteur de gaz correspondant à cette application est conçu et fabriqué conformément à la série IEC 61508. La fourniture, l'application, l'intégration et le fonctionnement de cette application sont couverts par la présente Norme.

A.1.3 Application 3

Cette application couvre l'utilisation d'un système fixe de détection de gaz qui agit comme un sous-système d'un système intégré plus important (voir la Figure A.1). Ce sous-système est ensuite intégré à un système de commande DCS ou ESD. Le système de commande DCS ou ESD réalise la logique du système final et lance l'action de sécurité.

Le sous-système fixe de détection de gaz correspondant à cette application est conçu et fabriqué conformément à la série IEC 61508. La fourniture, l'application, l'intégration et le fonctionnement de cette application sont couverts par la présente Norme.

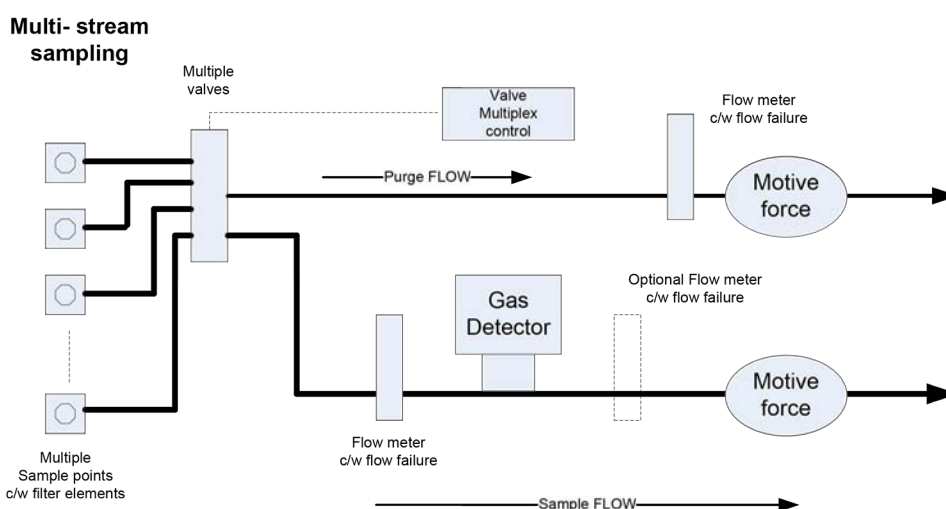
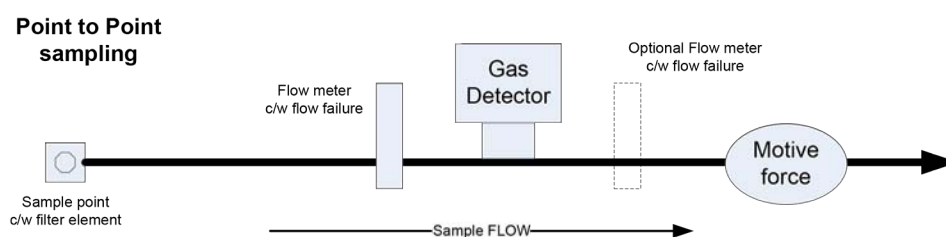
A.1.4 Application 4

Cette application couvre l'utilisation d'un système fixe de détection de gaz complet qui agit comme un système de sécurité complet (voir la Figure A.1).

Le système fixe de détection de gaz correspondant à cette application est conçu et fabriqué conformément à la série IEC 61508. La fourniture, l'application, l'intégration et le fonctionnement de cette application sont couverts par la présente Norme.

A.2 Applications typiques d'échantillonnage

A.2.1 Échantillonnage point à point



IEC 1062/14

Légende

Anglais	Français
Point to Point sampling	Echantillonnage point à point
Sample point c/w filter element	Point d'échantillonnage avec filtre
Flow meter c/w flow failure	Débitmètre avec défaillance de débit
Gas Detector	Détecteur de gaz
Sample FLOW	DEBIT de l'échantillon
Optional Flow meter c/w flow failure	Débitmètre optionnel avec défaillance de débit
Motive force	Force motrice
Multi-stream sampling	Echantillonnage multiflux
Multiple valves	Vannes multiples
Valve Multiplex control	Commande multiplex de vannes
Purge FLOW	DEBIT de purge
Multiple Sample points c/w filter elements	Points d'échantillonnage multiples avec filtres

Le système de commande multiplex de vannes doit faire partie du système de commande de détection de gaz ou être intégré au système de commande de détection de gaz pour garantir que toute alarme déclenchée par le gaz est attribuée au bon point d'échantillonnage (emplacement).

Figure A.2 – Configurations typiques d'aspiration de détecteur de gaz

Un système d'échantillonnage point à point comporte trois unités matérielles principales outre le détecteur de gaz (voir la Figure A.2). Ces trois unités sont:

- a) un point d'échantillonnage qui comprend normalement un filtre à particules ou équivalent;
- b) une indication de flux avec un signal (faible et/ou élevé) de défaillance simple ou double; et
- c) une "force motrice".

NOTE Une force motrice pourrait être une pompe électromécanique, un éjecteur d'air ou tout autre moyen permettant de prélever un échantillon de gaz.

Les trois unités matérielles sont connectées ensemble à l'aide d'une ligne d'échantillonnage. Il convient de choisir avec précaution le matériau de la ligne d'échantillonnage car certains matériaux peuvent être affectés par le gaz cible ou peuvent interférer avec lui. Le système d'échantillonnage point à point peut comporter un système de conditionnement d'échantillon, (non illustré ici).

Le débitmètre étiqueté "optionnel" positionné après le détecteur de gaz dans la Figure A.2 peut être une alternative à l'autre débitmètre ou peut être utilisé en complément de l'autre.

A.2.2 Échantillonnage multiflux

Un système d'échantillonnage multiflux comporte quatre unités matérielles principales outre le détecteur de gaz (voir la Figure A.2). Ces quatre unités sont:

- a) des points d'échantillonnage qui comprennent normalement un filtre à particules ou équivalent;
- b) un assemblage de plusieurs vannes et un contrôleur multiplex de vanne;
- c) une indication de flux accompagnée d'un signal (faible et/ou élevé) de défaillance simple ou double pour la ligne d'échantillonnage et une indication de flux accompagnée d'un signal (faible et/ou élevé) de défaillance simple ou double pour la ligne de purge; et
- d) une "force motrice".

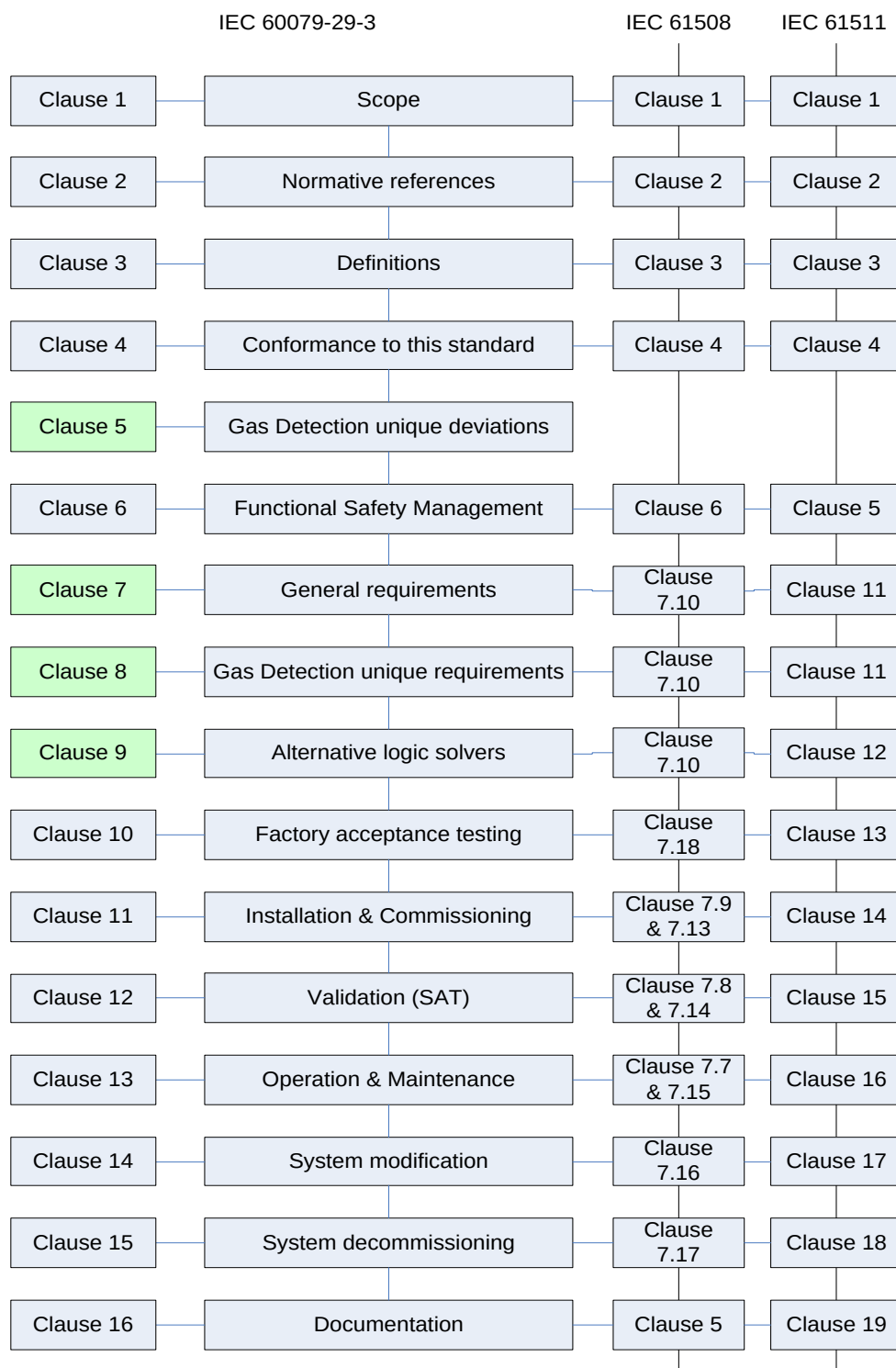
NOTE Une force motrice pourrait être une pompe électromécanique, un éjecteur d'air ou tout autre moyen permettant de prélever un gaz échantillon, avec une force motrice séparée pour la purge des lignes d'échantillonnage.

Les quatre unités matérielles sont connectées ensemble à l'aide de lignes d'échantillonnage et de purge. Il convient de choisir avec précaution le matériau de la ligne d'échantillonnage car certains matériaux peuvent être affectés par le gaz cible ou peuvent interférer avec lui. Le système d'échantillonnage multipoints peut inclure un système de conditionnement d'échantillon (non illustré ici). Il convient de relier le système de commande multiplex de vannes au système de détection de gaz pour s'assurer que l'échantillon de gaz analysé correspond à l'emplacement du point sensible dans la logique de l'unité de commande de détection de gaz.

Le débitmètre étiqueté "optionnel" positionné après le détecteur de gaz dans la Figure A.2 peut être une alternative à l'autre débitmètre ou peut être utilisé en complément de l'autre.

Annexe B (informative)

Références croisées entre normes



IEC 1063/14

NOTE Les articles mentionnés dans la Figure B.1 sont reliés aux éditions de l'IEC 61508:2010 et de l'IEC 61511:2003.

Légende

Anglais	Français
Clause 1	Article 1
Scope	Domaine d'application
Normative references	Références normatives
Definitions	Définitions
Conformance to this standard	Conformité à la présente Norme
Gas Detection unique deviations	Ecartés spécifiques à la détection de gaz
Functional Safety Management	Gestion de la sécurité fonctionnelle
General requirements	Exigences générales
Gas Detection unique requirements	Exigences spécifiques à la détection de gaz
Alternative logic solvers	Unités logiques alternatives
Factory acceptance testing	Essais de réception en usine
Installation & Commissioning	Installation & mise en service
Validation (SAT)	Validation (SAT)
Operation & Maintenance	Exploitation & Maintenance
System modification	Modification du système
System decommissioning	Déclassement du système
Documentation	Documentation

Figure B.1 – Références croisées entre normes

Annexe C (informative)

Transformation des exigences

C.1 Généralités

La présente annexe tente d'établir un rapport entre les contraintes de la norme générique (série IEC 61508), des autres normes d'application (série IEC 61511) et des autres normes de sécurité et les exigences applicables à un système fixe de détection de gaz, c'est-à-dire les exigences de la présente Norme internationale.

"Caractéristique" illustre la philosophie de base de la sécurité fonctionnelle. "Transformation" illustre l'interprétation spécifique correspondant aux systèmes fixes de détection de gaz.

En ce qui concerne les équipements non couverts par la présente Norme internationale, il convient, pour définir les exigences spécifiques, de suivre la philosophie de la présente annexe.

De plus, il convient d'utiliser les tableaux de l'IEC 61508-2 et l'IEC 61508-3 et la présente annexe pour déterminer la capacité SIL de ces équipements.

C.2 Capacité SIL 1

C.2.1 Caractéristique

Il convient de concevoir, de fabriquer et de mettre en œuvre les équipements utilisés pour une fonction de sécurité dans un système approprié de gestion de la sécurité qui inclut les exigences de vérification, d'évaluation de la sécurité fonctionnelle et de compétence. Le calcul de la proportion de défaillances en sécurité n'est exigé que pour les modules complexes (comme spécifié dans l'IEC 61508-2).

Sélectionner les composants, par exemple l'application de composants validés, permet d'éviter les défauts. Les parties pertinentes pour la sécurité du système sont vérifiées à intervalles réguliers. L'occurrence d'un défaut peut provoquer la perte de la fonction de sécurité.

C.2.2 Transformation

Il convient que le système ait démontré sa conformité à l'IEC 60079-29-1, à l'IEC 60079-29-4 ou aux autres normes métrologiques et qu'il soit maintenu conformément aux instructions du constructeur. Outre les normes métrologiques, les exigences pour la sécurité fonctionnelle des sorties d'alarme, pour l'alimentation et les conditions d'état spécial sont indiquées. Il convient d'effectuer un contrôle de vraisemblance de l'entrée utilisateur, par exemple, il convient que le réglage des niveaux d'alarme ne soit possible que dans l'étendue de mesure.

Il convient que tous les équipements soient configurés de sorte qu'en cas de perte de l'alimentation, un état spécial ou une condition de défaut est réalisé et un état connu est initié. L'initiation d'un état de sécurité peut être automatique ou manuelle en réponse à tout type de condition d'alarme.

Pour les équipements qui dépendent du logiciel pour satisfaire aux exigences de fonction de sécurité, il convient que le logiciel soit conforme aux exigences de l'IEC 61508-3 pour la capacité SIL 1.

C.3 Capacité SIL 2

C.3.1 Caractéristique

Pour les équipements simples, on suppose que la proportion de défaillances en sécurité se situe entre 60 % et 90 % si la tolérance aux anomalies du matériel est de 0 (IEC 61508-2). Pour les équipements complexes, il convient que la proportion de défaillances en sécurité se situe entre 60 % et 90 % si la tolérance aux anomalies du matériel est de 1 ou il convient qu'elle se situe entre 90 % et 99 % si la tolérance aux anomalies du matériel est de 0 (IEC 61508-2).

Les équipements comportent les moyens de vérifier à intervalles réguliers toutes les fonctions nécessaires pour obtenir les fonctions de sécurité exigées par le système de détection de gaz.

C.3.2 Transformation

Outre la capacité SIL 1, il convient que des dispositifs d'autotest pour le matériel et le logiciel soient disponibles à chaque période de démarrage et sur demande de l'utilisateur. Il convient d'inclure dans le plan de maintenance la vérification de toutes les parties relatives à la sécurité. Selon l'application, des procédures opérationnelles supplémentaires sont exigées, par exemple, il convient de considérer des intervalles d'étalonnage plus courts ou le remplacement des filtres dans des conditions environnementales sévères. Il convient d'indiquer et de signaler par une alarme les états spéciaux qui sont activés automatiquement en fonctionnement normal du système fixe de détection de gaz. Il convient de pouvoir vérifier les réglages des paramètres en mode opérationnel.

Pour les équipements qui dépendent du logiciel pour satisfaire aux exigences de fonction de sécurité, il convient que le logiciel soit conforme aux exigences de l'IEC 61508-3 pour la capacité SIL 2.

C.4 Capacité SIL 3

C.4.1 Caractéristique

Pour les équipements simples, on suppose que la proportion de défaillances en sécurité se situe entre 60 % et 90 % si la tolérance aux anomalies du matériel est de 1 ou il convient qu'elle se situe entre 90 % et 99 % si la tolérance aux anomalies du matériel est de 0 (IEC 61508-2). Pour les équipements complexes, il convient que la proportion de défaillances en sécurité se situe entre 90 % et 99 % si la tolérance aux anomalies du matériel est de 1 ou il convient qu'elle soit ≥ 99 % si la tolérance aux anomalies du matériel est de 0 (IEC 61508-2).

Il convient que l'occurrence d'un seul défaut ne provoque pas la perte de la fonction de sécurité. L'accumulation de défauts non détectés peut provoquer la perte de la fonction de sécurité car les éventuels défauts ne sont pas tous détectés.

C.4.2 Transformation

Outre la capacité SIL 2, il convient de concevoir les parties relatives à la sécurité du système de détection de gaz, y compris les signaux de sortie, de sorte qu'une seule défaillance ne provoque pas une perte de la fonction de sécurité. Dans toute la mesure du possible, il convient de détecter une seule défaillance.

Pour les équipements qui dépendent du logiciel pour satisfaire aux exigences de fonction de sécurité, il convient que le logiciel soit conforme aux exigences de l'IEC 61508-3 pour la capacité SIL 3.

Bibliographie

IEC 60079-10-1, *Atmosphères explosives – Partie 10-1: Classement des emplacements – Atmosphères explosives gazeuses*

IEC 61511-1, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus – Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel*

IEC 61511-2, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de la CEI 61511-1*

IEC 61511-3, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

ISA-TR84.00.07, *Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness* (disponible en anglais seulement)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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