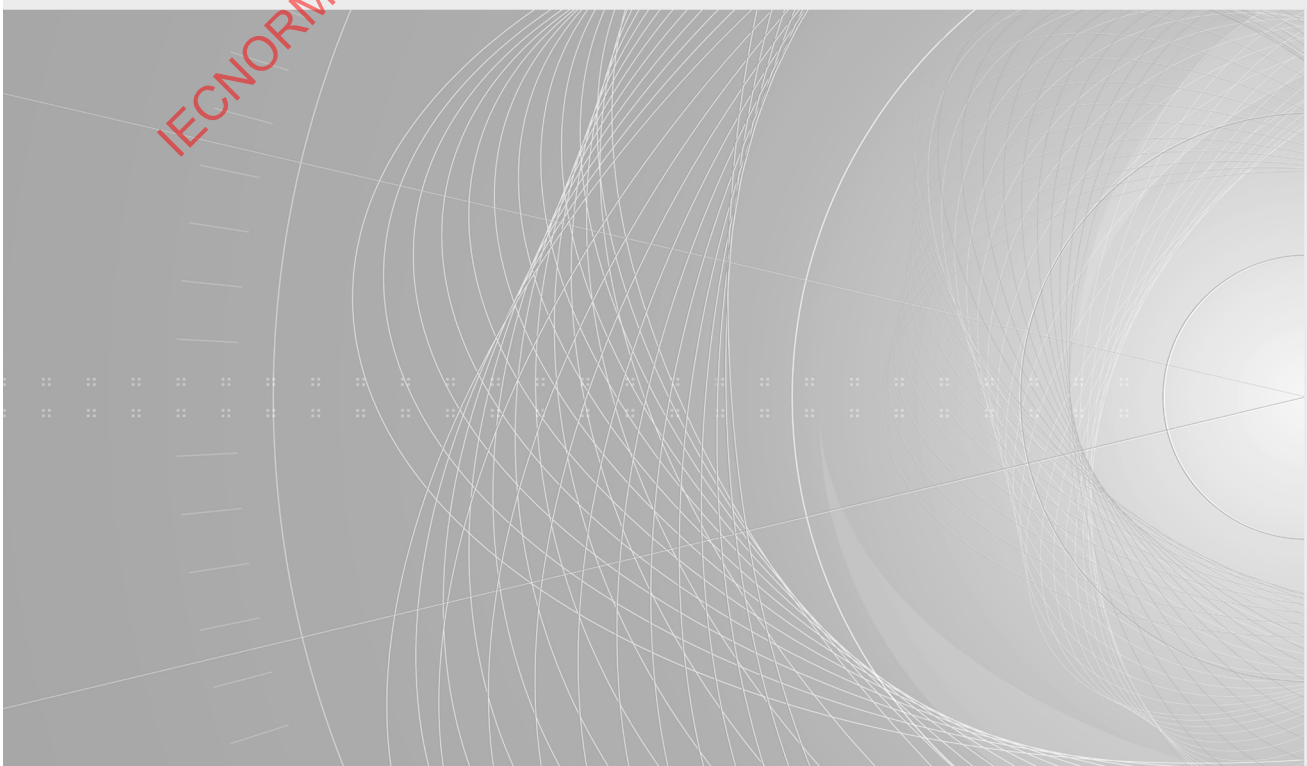
IEC TR 63176

Edition 1.0 2019-01

TECHNICAL REPORT

Process analysis technology systems as part of safety instrumented systems



IEC TR 63176:2019-01(en)

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 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 TR 63176

Edition 1.0 2019-01

TECHNICAL REPORT

Process analysis technology systems as part of safety instrumented systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.40

ISBN 978-2-8322-6407-2

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

PROCESS ANALYSIS TECHNOLOGY SYSTEMS AS PART OF SAFETY INSTRUMENTED 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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63176, which is a Technical Report, has been prepared by subcommittee 65B: Measurement and control devices, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
65B/1111/DTR	65B/1131/RVDTR

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

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

This Technical Report is designed as a recommendation to aid users of process analyzer technology that measures installations as part of safety instrumented systems and should be treated exclusively as a recommendation. Formulations of a binding character encountered in the recommendation are due to the safety-related content. However, the advisory character of this document is maintained as a whole. Process analyzer technology measuring equipment is used, for example, in the process industry as sensor components of safety instrumented systems. In many cases, they represent the only or most efficient method for monitoring a process variable, which, for its part, enables a reliable evaluation of designated use of the system to be protected. Owing to the direct material interaction with the process medium, process analyzer technology measuring equipment is in general more susceptible to failure and requires more maintenance than the sensors widely used for pressure, temperature, filling level and flow measurement. A consequence of this interaction is the inability to avoid systematic failure completely. This problem is usually countered by checking the measuring equipment at short, regular intervals.

The variety of process analytical measurement variables and methods and, consequently, the comparatively limited number of process analyzer technology measuring devices used in each case for a single, precisely limited, application makes a quantitative evaluation of functional safety in accordance with IEC 61511 difficult in most cases. Beside the often-inadequate specifications of manufacturers for evaluating components as safety instrumented systems, there are an insufficient number of comparable applications. However, several hundred safety instrumented systems have been successfully realized in the last 30 years among the process analyser community using process analyzer technology measuring equipment.

Measures are proposed in areas where normative requirements cannot be fulfilled, or only inadequately. These measures lead to an equivalent level of safety when applied carefully.

Requirements concerning functional safety of electrical and electronic systems are described in IEC 61508, specified for “Safety instrumented systems for the process industry sector” in the sector standard IEC 61511. The aim of this document is to describe a procedure for the use of process analyzer technology measuring devices as part of safety instrumented systems in a guideline.

PROCESS ANALYSIS TECHNOLOGY SYSTEMS AS PART OF SAFETY INSTRUMENTED SYSTEMS

1 Scope

This document encompasses recommendations for planning, installation and operation (incl. maintenance) of process analyzer technology measuring equipment in process industry safety instrumented systems. It covers all necessary steps for the qualification of safety equipment and supplements the safety management of safety instrumented system equipment through the addition of special requirements for process analyzer technology equipment. This document does not encompass the entire safety management of safety instrumented system equipment.

The term “qualification” used in this recommendation refers exclusively to the testing of the suitability of the process analyzer technology system for use in a safety instrumented system device. It is different from the term "qualification" used in the pharmaceutical environment.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61511-1:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*

IEC 61326-3-1:2017, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

IEC 61326-3-2:2017, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
PAT measuring equipment
process analysis technology systems as entirety of all equipment and media necessary for realization of the substance-related measurement function

Note 1 to entry: An exemplary, but not necessarily complete list includes sampling equipment, sample conveying equipment, sample conditioning equipment, sample recirculation equipment, the analyser, PAT control units and infrastructural equipment such as supply, reference and calibration media and the necessary power supply. From case to case, a required cabinet or the location in an analyser house or room should be included.

3.1.2
basic testing
possible preselection of suitable analytical equipment for safety instrumented systems without any reference to a specific measuring task

Note 1 to entry: This applies exclusively to the testing of analytical equipment according to the criteria mentioned in Annex A.

3.1.3
application testing
test that ensures that the measuring task can be successfully realized with the PAT system

Note 1 to entry: This includes checking the configuration and, occasionally, programming of analytical equipment to correspond to the measuring task, taking the influence of sample processing into consideration, especially its accuracy, determining the influences of the matrix and state variables (pressure, temperature, flow), both of the medium and the analytical equipment environment, and knowledge of the stability over time.

3.1.4
operational experience
knowledge available prior to using an analyser, including the required accessories for comparable measuring tasks

Note 1 to entry: It therefore involves exclusively experience gained through actual use of comparable analytical equipment for comparable measuring tasks.

3.1.5
in-service testing
monitored operation of the PAT system as part of a safety instrumented system during production operation

Note 1 to entry: An explicit differentiation is made here between the procedure in the case of proven operational performance of PAT systems and the corresponding procedure for safety instrumented system equipment.

Note 2 to entry: The test work to be realised, the timetable, specifications for the evaluation of results, additional measures for the fulfilment of the safety function required from case to case during in-service testing and the responsible personnel in this phase should be documented.

3.1.6
proven performance
entirety of knowledge that is part of the final decision in favour of or against the suitability of a proposed process analyser installation as part of a safety instrumented system

Note 1 to entry: Proven performance will be achieved by sufficient operation experience including approvement of suitability of the measuring task. If not practicable, proven performance can be achieved through in-service testing.

Note 2 to entry: Proven performance of PAT is finally determined by a team of experts and differs in the manner of its determination from the method usually used for field devices and PLCs.

3.1.7
calibration
inspection task, its purpose being to confirm the target condition

Note 1 to entry: "Calibration" means determining and documenting the deviation of displayed value of a measurement from the correct value of the measurement.

Note 2 to entry: When calibrating a process analyser, the relationship between input and output is determined and documented under specified conditions. Input value is the physical quantity to be measured. Output value is the electrical output signal of the measuring device.

3.1.8
adjustment
setting or modification of an instrument in order to eliminate systematic errors as far as it is necessary for the intended application

Note 1 to entry: Adjustment is the process by which a meter is set or adjusted so that the measurement errors are as small as possible from the nominal value and are within the device specifications. This adjustment is a process that changes the instrument permanently.

3.1.9
test interval
PAT systems as part of safety systems are subject to different test intervals for proof testing with differing degrees of testing

Note 1 to entry: Examples being the following:

- Test interval for an internal PAT system diagnostic sensor (e.g. the flow meter)
- Test interval for an internal PAT system channel (e.g. automatic calibration)
- Test interval for an internal PAT system channel (e.g. inspection and servicing incl. manual adjustment)
- Test interval for the entire system (manual, PAT + rest of safety instrumented systems)

3.1.10
proof test
test for discovering errors in a technical safety system so that the system, if necessary, can be returned to the condition in which it fulfils its intended function

3.1.11
proof test coverage
coverage of test for discovering errors in a technical safety system

Note 1 to entry: This term originally referred to the proof test. However, any test (see test interval) can, in principle, achieve a coverage <= 1. For sensors, this means that the DU failure rate of the channel increases due to non-function, while the DD rate decreases. Automatic calibration can usually only check a certain DU rate at adequately brief time intervals. It can also not be ruled out that channel failures will remain undetected during inspection and maintenance. Careful planning of test processes should ensure that there is only a low probability of this occurring.

3.2 Abbreviated terms

DC	diagnostic coverage
DD	dangerous detected
DU	dangerous undetected
FAT	factory acceptance test
FMEA	failure mode and effects analysis
FMEDA	failure mode, effects and diagnostic analysis
HazOp	hazard and operability study
HFT	hardware fault tolerance
PAT	process analyser technology
PFD	probability of failure on demand

PID	piping and instrumentation diagram
SAT	site acceptance test
SIF	safety instrumented function
SIL	safety integrity level
SIS	safety instrumented system
SFF	safe failure fraction
PTC	proof test coverage
λ_i	failure rate of i component
μ_i	repair rate of i component
$U_{DD,\ i}$	unavailability through DD failure of i component
$U_{DU,\ i}$	unavailability through DU failure of i component
U_{ch1}	unavailability of channel 1
U_{MooN}	unavailability of entire system in the moon configuration
β	proportion of common cause failures
T_{max}	maximum test interval
PFD_{beta}	proportion of pfd value due to common cause
PFD_{MooN}	pfd value of entire system without taking common cause into consideration
PFD_{PAT}	pfd value of the entire pat system

4 Qualification process

4.1 Overview

PAT measuring devices are generally complex SIS sensors individually tailored to suit the specific requirements of the process engineering process and which describe the condition of the process through measurement of the concentration of one or more substances.

The individuality of these sensors often makes it impossible to transfer operational experience with a sufficient number from existing SIS to new PAT measuring equipment which is to be planned. In-service testing of completed functional measuring equipment should be conducted in these cases. The individuality of these measuring devices requires a high degree of technical competence on the part of those involved in the process at all levels of the qualification process described (see Figure 1). This includes (installation) constructors and operators of the PAT system (see 4.2 and 4.3). Each qualification step will be documented

The qualification process will be performed by PAT-experts under participation of safety engineers for process control and process engineering. All relevant process data for the PAT-System performance will be confirmed by the responsible safety engineer.

Where several measuring methods are technically practical, these methods should be examined and assessed. Further aspects to reduce/minimize the overall failure probability of the PAT system should be considered right from the beginning of planning, including:

- the degree of redundancy/fault tolerance;
- homogeneous or diverse redundancy;
- operational experience/proven performance from other measuring equipment;
- risk associated with the metrological application (e.g. cross-sensitivities, ageing processes, common cause failure).

Metrological suitability can be ascertained from experience in earlier applications or is proven in the context of an application test.

When using redundant systems, delta deviation monitoring of the measured values should be considered.

Selection of the measuring method is followed by design of sample conditioning and determining of components relevant to this. Both the design and choice of components should be justified where this is relevant to functionality and documented. Appropriate and reliable equipment and components should be used for constructing the PAT measuring system. Verification of reliability is usually based on the operational experience of the operator, but can also be realized through a reliability assessment conducted by the manufacturer.

Assumptions of the (installation) constructor and/or plant operator specific to the application (e.g. failure rates, proof test intervals, etc.) always take precedence over manufacturer specifications. The constructor and/or operator are responsible for the SIL classification appropriate for the application, regardless of any possible manufacturer recommendation. Although preference should be given to the use of SIL-certified analysers, this does not mean it is mandatory to use an analyser SIL-certified by the manufacturer. Consequently, an analyser without SIL certification can be used in preference to a SIL-certified analyser.

It is also unnecessary to realize a specific application exclusively with an analyser approved for this purpose by a particular manufacturer. For example, there is no reason why an analyser certified as SIL1 by the manufacturer and with proven performance should not be used in a 1-channelled SIL2 application if the qualification process is realized.

A detailed examination of the overall PAT system should be conducted in the case of PAT measuring equipment. The aim here is to detect potential failures, evaluating these with regard to the effect on functional safety. Appropriate measures for failure control, failure avoidance, failure detection or the reduction of failure frequency can be derived from this. The PFD value should be estimated. Options for estimation are mentioned in 4.5.6. The PFD value of PAT is taken into consideration in the overall PFD value for SIS.

Where proven performance, an adequate HFT value (see 4.5.5) and a PFD value (see 4.5.7) are available, the suitability of the PAT system for SIS should be assessed as a final measure.

An SFF is inadequate, owing to the complexity of process analyser equipment. For this reason, the SFF is neither evaluated nor indicated in the case of process analyser technology systems.

Where adequate data is still not available to establish proven performance, but measuring methods are already being used with great success in media of a comparative type, the suitability of the PAT system as part of a SIS safety installation during active operation can be determined based on the documented in-service testing process (see 4.5.8).

As a result of the in-service testing process, the operator may be faced with requirements that need to be met to maintain functional safety. Finally, the life cycle of PAT measuring equipment should be documented from commissioning to decommissioning.

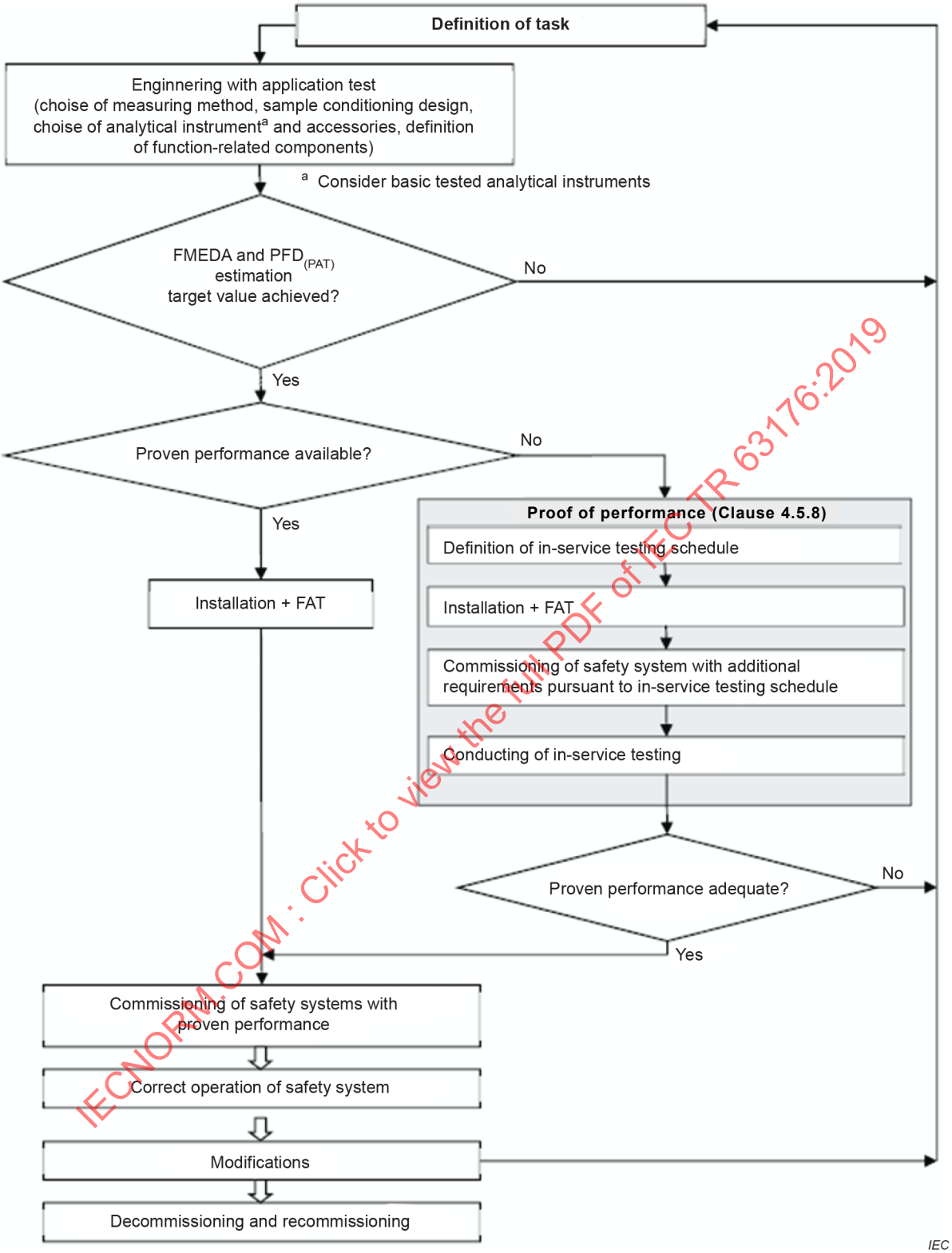


Figure 1 – Qualification process levels for a PAT measuring system

4.2 Recommendation for constructor requirements

The following requirements are derived from IEC 61511-1:2016, 5.2 and set out in concrete terms to address process analyser technology issues. Verification of qualification of a PAT installation as part of a SIS demands comprehensive knowledge and experience in the area of process analyser technology and its use in chemical and/or physical processes. This knowledge and experience can be compiled in an expert team, which realizes verification of

qualification. Persons, departments or organizations involved in the implementation of measures in the safety life cycle should be competent to realize the tasks for which they are responsible. Those responsible for the qualification process require adequate management and leadership qualities for the respective task and an understanding of the consequences of any event which may occur. New and complex applications or technologies should only be used if the team is capable of understanding these and evaluating the safety aspect.

The following knowledge and experience should be available in the expert team:

- Knowledge of relevant chemical or physical process steps at the measuring location

  The physical and/or chemical parameters at the measuring location should be known for assessing the suitability of an analyser in a chemical or physical process (i.e. evaluation of the suitability of an analyser in an application). This data should be taken into consideration in the entire range of correct operation (acceptable range and permissible failure range) right up to the limit of incorrect operation. Start-up and shutdown should be taken into consideration in the same manner as regular production operation if this is not explicitly exempted from the safety function.

- Experience in the preparation of applications for the analyser

  An understanding of a certain measuring method and its limits from a physical and chemical point of view is necessary to prepare an application for an analyser method for use in SIS.

- Experience in the design of sample conditioning processes

  Knowledge of the system components in a sample conditioning process, engineering of sample conditioning processes, the physical and chemical properties of the sample and the measuring process are necessary to evaluate the suitability of a sample conditioning process.

- Knowledge of working methods in safety engineering

  Competence in conducting FMEDA, estimating the PFD value of the PAT system and the competence to cooperate in risk analysis (e.g. HazOp method for prognosis, identification of cause, estimation of effects and countermeasures) is necessary.

- Knowledge of applicable codes and standards

  Relevant codes and standards when it comes to design at the time this document was compiled are IEC 61508 and IEC 61511.

4.3 Recommendation for plant operator requirements

The following requirements are derived from IEC 61511-1:2016, 6.2 and set out in concrete terms to address process analyser technology issues. The operator of a PAT installation as part of a PLT safety system should ensure throughout the entire life cycle that the required safety integrity level of the safety function in question is sustained during operation and maintenance. If the SIS is to be operated and maintained in a manner that sustains the required functional safety, it is necessary to provide the competence necessary for the maintenance of such systems at all levels of maintenance or to entrust maintenance to a service provider with the appropriate competence. The organizational form is not predetermined.

In addition to the requirements described in IEC 61511, this competence encompasses the following additional knowledge, skills and experience:

- Knowledge of the PAT system functionality

  Knowledge of the correct function of the PAT system, particularly sample conditioning. Understanding of the principles underlying the measuring method. Knowledge of the functional limits of the measuring system usually drawn from the ambient conditions and the interaction with the measuring medium.

- Skill and experience in the maintenance of PAT equipment

Skill in mechanical and electrical work on the PAT measuring system. This includes both servicing and maintenance work. Experience in the identification of failure (i.e. the occasional failure of the measuring system to function correctly).

4.4 Basic testing (analyser only)

Each analyser used in a safety system should meet fundamental quality requirements. Basic testing can contribute to the examination of these quality requirements (see Annex A). Basic testing does not replace the application testing of the analyser, which, additionally, will be conducted with respect to the sample conditioning system in question, or proven performance.

As the results of basic testing are determined by the hardware and software of an analyser, it should be ensured that the manufacturer reports changes to the hardware or software proactively and immediately to the end-user. The plant operator should thereafter decide on the updating of basic testing from case to case. Basic testing need generally not be updated if the manufacturer has developed the analyser in compliance with the quality requirements of IEC 61508.

4.5 Engineering

4.5.1 General

The engineering of a PAT measuring installation as part of a SIS should be realised with extreme care, as this decisively influences the availability of the SIS safety instrumented system in later operation.

Fundamentally speaking, the engineering of a PAT system should be based on specification worksheets that include process data with all physical and chemical properties (pressure, temperature, composition, phase, dew point, etc.).

Process analyser technology systems are generally more complex in their structure than other measuring systems (e.g. for pressure, temperature or flow). This applies in particular to so-called online measuring systems, which remove a representative part of a substance mixture in the production process and condition it for subsequent analysis. This could alter the substance mixture in its composition through components such as valves, pumps, coolers, separators and filters. Equally, a situation could arise where the sample can no longer be conveyed to the analyser, or not quickly enough, and the measurement value no longer meets the requirement for contemporary data. Sample conditioning is therefore an integral part of the SIS safety system and, consequently, should be taken into consideration during the course of PFD determination.

Sample conditioning can, under certain circumstances, strongly influence the PFD value of sensor installations in the PAT system. PAT systems are for this reason equipped where possible with additional sensors which can identify sample conditioning errors in the shortest possible time. The proportion of dangerous undetected failures present can be reduced as a result by transforming these into detected failures.

In addition to proof testing, PAT systems are, in comparison to conventional safety systems, subjected to further manual testing and calibration at shorter intervals, including adjustment from case to case where necessary. Manual or automatic calibrations without adjustment between the aforementioned manual testing can contribute to the plausibility testing of the PAT system.

As the correct functionality of the additional sensors is decisive for the proportion of hazardous undetected and detected failures, these are monitored in separate testing intervals where appropriate.

4.5.2 Design data

The principles underlying the engineering of a PAT measuring installation as part of a SIS are:

- Definition of the SIF

  The performance level of functional safety (e.g. SIL). This is realized in the corresponding safety evaluation/risk analysis of the production line and documented. The aim here is to limit a particular condition parameter of a process. In PAT, this usually involves limitation of the concentration of a defined substance upwards or downwards.

- The max. permissible response time of the safety system

  This should be taken into consideration during design of the PAT and is dependent on the sample lag time (i.e. sample collection, transport and analysis period), response durations of the actuators and logical components.

- Process engineering data at the sampling point.

  This includes the composition of the sample to be analyzed and the physical/technical data of the material flow at the sampling point, incl. toxicity and corrosivity. The influence of special system conditions (e.g. start-up, shutdown, load change, malfunction) should be taken into consideration in this context.

4.5.3 Analyser including application

Selection of the measuring principle and analyser can be based on the design data. Preference in the selection of analysers should be given to those whose basic suitability has been determined in Annex A.

The specific metrological suitability can be ascertained through experience with comparable existing applications. However, it is generally verified during the analyser application.

The reasons for the selection of the method and analyser should be documented.

4.5.4 Sample conditioning

Sample conditioning required from case to case is determined by the design data and the analyser selected.

Sample conditioning should preferably involve diagnostic functions so that failures that influence the safety function can be identified and signalled (avoidance of DU failures and transformation of DU failures into DD failures).

The periphery should, where possible, encompass components with proven operational reliability.

The complete system (PAT measuring installation) consisting of sample conditioning and analyser should be illustrated in a P&I diagram (analyser flow sheet) with a parts list.

4.5.5 HFT

The HFT provides information on the degree of redundancy of a system. Derived from IEC 61511-1:2016, 11.4, the following hardware fault tolerances in Table 1 apply:

Table 1 – Minimum HFT requirements according to SIL

SIL	Minimum hardware fault tolerance during in-service testing	Minimum hardware fault tolerance in case of adequately proven performance
1	0	0
2	1	0
3	2	1

Proven performance is always necessary for PAT systems in SIS (see Clause 4). This corresponds to selection on the basis of an earlier application (IEC 61511-1:2016, 11.5).

The minimum hardware fault tolerance in the case of adequately proven performance may only be applied if only process-related parameters can be configured in the PAT system and this setting is protected. Editing of the PAT system or analyser software during proof of performance should be explained and documented. The proof test should be restarted.

4.5.6 Failure mode effects and diagnosis analysis of the PAT system (FMEDA)

An analysis of the failure probability and effects should be conducted for the entire PAT system, including supply, comparative and auxiliary media (e.g. FMEDA – failure mode, effects and diagnostic analysis). The failures observed during this should be described and appropriately classified (e.g. DD – dangerous detected, DU – dangerous undetected, S – safe) and failure rates listed (including common cause, common mode) with details of their origin (e.g. manufacturer specification, own statistics). Potential failures are identified by the expert team and their failure rates determined. The failures identified should be further classified in stochastic and systematic. Systematic failures should be remedied where possible. Where this is not possible, systematic failures should be identified by diagnostic devices. Efforts should be made to achieve a proof test coverage rate of 100 % for regular examination of the PAT system (proof test). Where the proof test coverage rate is estimated lower, this conservative estimated value should be documented and justified. Statistical processing of individual failure rates does not appear to be practical owing to the estimation inaccuracy involved. All relevant correct operating conditions should be observed.

The scope of the FMEDA depends on the complexity of the PAT system. An example of the documentation of a weak point analysis of this kind is illustrated in Annex B.

On the other hand, human error (e.g. use of unsuitable auxiliary media) is not taken into consideration. This failure should be ruled out through organisational measures. Likewise, failures arising from, for example, the systematic inaccuracy of the concentration of test gases are not taken into consideration in the FMEDA, but should be considered in another suitable manner, for example, by shifting the switching point.

4.5.7 Estimation of the PFD_{PAT} value

The PFD_{PAT} value is used to estimate the probability of failure on demand of the PAT measuring system. The PFD_{PAT} value only represents part of the PFD of the safety system. In all cases, further PFD rates should be taken into consideration in the overall evaluation (e.g. logic or actuator-related). The PFD_{PAT} rate can be minimised in some cases through additional status signals (transformation of DU failures into DD failures) and/or reduction of maintenance intervals. Where this is no longer possible, the measuring system should be changed where necessary or the number of channels increased. The final identification of an excessive PFD_{PAT} rate excludes the measuring installation in question as part of the SIS.

The PFD_{PAT} value should be determined with a suitable process. One method, the numerical discrete method is illustrated below in an exemplary fashion.

The numerical discrete method for determining the PFD value, using spread sheet analysis, is realized on the basis of the unavailability of subcomponents of a system depending on time t. Cases of component-related unavailability can be suitably overlapped to create overall system unavailability. The PFD value is determined through averaging of this unavailability $U(t)$ over the system lifetime or the longest periodicity of the curve progression occurring.

Potential faults are first recorded through a failure mode, effects and diagnostic analysis (FMEDA) and classified as safe, dangerous detected and dangerous undetected. These faults form the basis for the cases of unavailability.

The formulae for unavailability $U(t)$ of components are universally valid and form the basis for the formulae used for calculating the PFD value contained in IEC 61508-6.

The method is described in Annex C.

4.5.8 Proven performance – from case to case following prior in-service testing of the PAT system

Proven performance will be achieved by sufficient operation experience including approvement of suitability of the measuring task. If not practicable, proven performance can be achieved through in-service testing.

Following the completion of the material flowchart, the parts list and estimation of the PFD_{PAT} value as adequate, a decision should be reached on whether adequate operational experience with a comparable PAT measuring system is available. It is up to the aforementioned team of experts to determine that operational experience is adequate or, where appropriate, to request an in-service test of the PAT measuring system. This is realised at the intended measuring location during all operating conditions. In-service testing should be conducted under the following conditions:

- It is foreseeable that in-service testing can be completed with a positive result.
- The PFD_{PAT} value estimated is adequately low (i.e. a considerable reserve of unexploited failure probability remains for the involvement of logic and actuator systems). Proof of performance through in-service testing should not occur if the maximum possible PFD value should already be assumed to be practically achieved during planning.
- Parts of the planned process analyser technology should already be successfully in use at a comparable position.
- The safety function should be supplemented from case to case through additional measures during the in-service testing phase.
- The in-service testing process and assessment criteria for later determination of proven performance should be documented prior to commencing installation.
- Where it is finally impossible to verify proven performance, the safety function should be guaranteed in another manner and through methods other than those of process analyser technology where necessary. This means that PAT is an unsuitable method in this case.

A new analyser or new sample conditioning can be established as the safety function with the aid of in-service testing (4.5.8).

4.5.9 Safety logic in the PAT system

The PAT systems as part of SIS installations examined here may have their own logic units which, for example, facilitate measuring point switchover or link signals in advance.

In principle, the logic component can be realised in the master control system or a superordinate safety-related PLC or a logic solver, laid in a separate PAT controller (PLC, safety-related PLC or logic solver) or contained completely in the analyser. Mixed forms are also possible.

Where safety-related information is processed separately, it is important to proceed in line with the standards and guidelines of functional safety (e.g. use of a safety-related PLC).

4.5.10 Sample switching

Additional risks are associated with a measuring point switchover, and it should be considered as a source of error in all cases. Potential DU failures due to malfunctioning valves can be reset to DD failures from case to case using position indicators. Extensions of the response duration of the limit value relevant for triggering the safety system that are caused by the switchover should also be taken into consideration

4.5.11 Compilation of a plan for periodic inspections during the runtime

The frequency of periodic testing of the entire measuring system should be determined in the context of PFD value estimation. Ideally, these periodic testing should identify all potentially occurring DU failures and idle monitoring installations, including position indicators, level, flow, pressure or temperature limit sensors.

The degree to which periodic testing detects the failures described should be estimated. This proof test coverage should be taken into consideration during estimation of the PFD value.

The test intervals determined have a considerable effect on the PFD value.

4.6 Commissioning of the safety system

Commissioning is realised following installation and SAT in the case of documented proven performance. In the absence of proven performance, commissioning can be realised in conjunction with an in-service test. Operating and maintenance personnel should be trained.

4.7 Documentation of the qualification process

Documentation of the qualification process should encompass the following:

- excerpt of the operational/HazOp safety evaluation;
- process engineering data for analyses worksheet;
- analyser, specification worksheet;
- material flowchart (PAT P&I, PAT P&ID) with parts list;
- analysers/parts documentation (e.g. SIL certificates);
- PFD estimation incl. FMEDA protocol;
- SIS loop schematics diagram;
- function diagram;
- safety considerations relating to the measuring function;
- test specification;
- information for the operator on functional safety;
- maintenance schedule;
- the person responsible for verifying qualification signs;
- the names of expert team participants are listed;
- case to case in-service testing schedule and records during this phase.

5 Regular operation

5.1 General

All tasks mentioned in Clause 5 should be initiated by the operator of the safety system.

5.2 Periodic testing during runtime

The PFD value determined in 4.5.7 is directly dependent on the test intervals defined. Test intervals should therefore be observed and documented in the maintenance schedule.

The inspection should be recorded in a test report. A detailed procedure plan for conducting the inspection is recommended. This can depend on different operational phases and activities (e.g. during testing of a start-up phase).

Inspection of the entire system: sensors – logic systems – actuators should be coordinated and conducted where appropriate with the other tasks involved. IEC 61511-1:2016, 5.2.1 to 5.2.3 also apply.

The function of the safety system should be verified regularly on the basis of the tasks involved. The PAT system should be included in this.

5.3 Documents and records in operation

5.3.1 General

It is recommended that the plant operator keeps records based on defined schedules and regulations which indicate that periodic testing (see 5.2) is conducted in the manner laid down during the planning phase. IEC 61511 provides the basis for this documentation.

These records should at least contain the information below.

5.3.2 Maintenance schedule

The maintenance and inspection schedule (M+I schedule) describes which work is to be performed in which interval. The M+I schedule contains at least the following information:

- measuring point number, safety function number;
- test interval;
- stipulation of the applied test specification.

The defined MTTR durations should not be exceeded, as the PFD value determined in 4.5.7 depends directly on these.

5.3.3 Working instructions

Conducting of inspections pursuant to the test specification (see 4.7) should be defined in working instructions.

5.3.4 Record of work realised

The following minimum content is recommended for the test report mentioned in 5.2:

- date of the inspection and maintenance work realised;
- name of the persons who realised the inspection and maintenance work;
- description of faults remedied (type);
- indication of the effected channels in the case of multichannel safety systems;

- clear marking of the system tested (e.g. measuring point number, safety function number);
- deviation from test interval;
- stipulation of the applied test specification;
- results of work and verification that the system has been recommissioned following maintenance without any faults.

5.3.5 Fault data recording

Every maintenance operation should be appropriately documented. The entire system, including sample conditioning, should be recorded in this respect. Subclause 5.3.4 applies correspondingly for the documentation.

Every device fault will be categorized as follows:

- fault location (process analyser, sample conditioning);
- fault detection (e.g. proof test);
- kind of fault (dangerous, safe);
- type of fault (random, systematic);
- cause of fault (e.g., process related, design fault, device fault, wrong calibration);
- details of fault (e.g., device type and manufacturer).

5.4 Evaluation of fault data and handling of deviations

In the context of a continuous improvement process, fault data should be evaluated between the operator of the production plant and PAT experts and deviations from correct operation minimised.

5.5 Modifications

5.5.1 Modifications to the PAT system

In the event of modifications to a safety system, there is a risk that systematic faults may be unwittingly or erroneously implemented that impair the desired behaviour of this safety system in a demand case. The PFD value is altered in this case, meaning that the criteria for the required SIL classification may no longer be met. The same system should be employed as in planning and installation of the existing safety system during evaluation of the modification. The responsible operating and maintenance personnel involved should be informed of the modification and trained where necessary with regard to the change.

Where components cannot be replaced 1:1 with identical spare parts, this is regarded as a modification and will be inspected. This applies to hardware and software. Software and hardware modifications undertaken by manufacturers on safety system components shall be reported by the manufacturer.

Renewed testing of software can be dispensed in case software has been developed pursuant to IEC 61508.

5.5.2 Modifications of the process engineering process

In the case of modifications to process engineering (chemical and physical) parameters or the materials used, the effect on suitability with regard to safety should be evaluated and documented. The same system should be employed as in planning and installation of the existing safety system. The original documentation is therefore in the possession of the operator.

5.6 Decommissioning and recommissioning

5.6.1 Decommissioning

Decommissioning is characterised by deactivation of supply and auxiliary power. Disconnection of the process alone does not represent the decommissioning of the PAT system.

5.6.2 Recommissioning

Recommissioning corresponds to initial commissioning. However, an in-service testing phase can be dispensed in case correct operation has not changed (see 5.5.2).

5.7 Grandfathering

In general, the usually used rules governing the safeguarding of existing standards apply. Specific process analyser engineering requirements should be taken into consideration in the event of modifications.

Annex A
(informative)

Basic testing of analysers

Basic testing relates exclusively to fundamental requirements with regard to the quality and operational characteristics of analysers intended for future use in safety installations subject to their technical suitability. Actual suitability for a particular measuring task is ensured through a task-related application test.

Contents of basic testing

1	**Organization check**
1.1	Type/Version
1.2	Measurement range, sensor
1.3	Serial no.
1.4	Hardware rev. no.
1.5	Software rev. no.
1.6	Documentation
1.6.1	Documentation version number
1.6.2	Comprehensibility
1.6.3	Correctness
1.6.4	Completeness
1.6.5	Operating and safety instructions in the local language
2	**Manufacturer specifications on analyser**
2.1	Development pursuant to IEC 61508 SIL2 or SIL3
2.2	EMC assured pursuant to IEC 61326-3-1 / IEC 61326-3-2
2.3	Failure rate DU
2.4	Failure rate DD
2.5	Failure rate SU
2.6	Failure rate SD
2.7	EC design pattern test certificate for measuring function
2.8	Permissible humidity
2.9	Ambient temperature range
2.10	Ambient temperature effect
2.11	Process temperature range
2.12	Process temperature effect
2.13	Process pressure range
2.14	Process pressure effect
2.15	Effect of vibrations
3	**Maintenance appraisal**
3.1	Design
3.2	Occupational safety
3.3	Operability
3.4	Capacity for resetting to default settings

3.5	Locking of parameterizing
3.6	Failure signal
3.7	Service request signal
3.8	Service signal
3.9	Maintenance outlay
3.10	Maintenance friendliness
3.11	Experienced data about manufacturer's devices subject to this appraisal
4	**Explosion protection appraisal**
4.1	Interlinking capability with other Ex-devices
4.2	Requirements in inspection certificates/operating manuals
4.3	Labelling of the device
4.4	EC design pattern test certificate and manufacturer’s declaration of conformity with regard to explosion protection
5	**Material compatibility appraisal**
5.1	Sensor
5.2	Containment (except sensors, elastomers and "windows")
5.3	Optical windows
5.4	Seals
6	**Inspections**
6.1	EMC testing pursuant to IEC 61326-3-1, IEC 61326-3-2
	Evaluation of faults with regard to safety function triggering
6.2	Linearity error – appraisal on the basis of a selected substance with regard to the max. deviation and max. hysteresis.
6.3	t_{90} – step response time
6.4	Signal attenuation at max. load

Figure A.1 illustrates the basic testing process for analyzers in PCT safety systems.

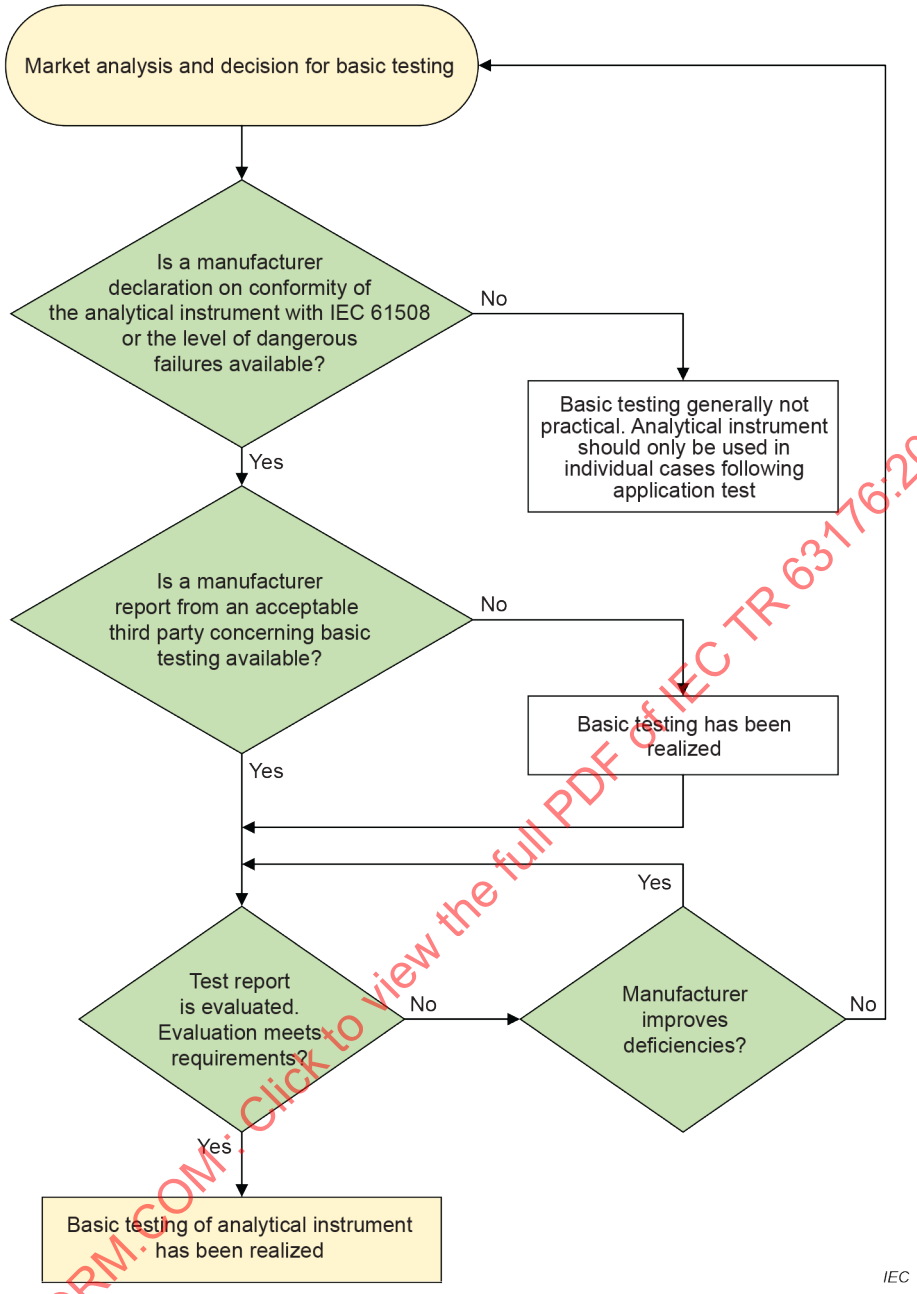


Figure A.1 – Basic testing process for analysers in SIS

Annex B
(informative)

FMEDA – documentation of safety assessment (example)

The following form (Figure B.1) can be used for systematic recording of potential failures and the status signals and maintenance intervals of a PAT system. Further parameters necessary for determining the PFD may arise, depending on the PAT system design.

PAT channel	Q 5551
Repair time (restoration time following malfunction) for a PAT channel [h]	72

Common Cause Factor	0.05

Maintenance parameters	**Test interval [h]**	**Test duration [h]**	**Diagnostic coverage [%]**
Safety instrumented System overall proof test interval	8760	4	100
PAT system channel [e.g. inspection and preventive maintenance interval *incl. manual adjustment*]	168	0,5	90
Part of PAT system channel [e.g. automated analyzer calibration interval]	24	0.05	50

	Automatic failure detection via			
Additional sensors	**No. 1**	**No. 2**	**No. 3**	**No. 4**
Name	FIA . 01 Sample	FIA . 02 Bypass	TIA*02 chiller	analyser diagnosis
Failure Rate [h]	1.2×10^{-4}	1.2×10^{-4}	5.8×10^{-5}	3.8×10^{-5}
sensor proof test interval [h]	24	24	720	168

Current Failure No.	**Failure description and effect on functional safety of PAT channel** [1]	**Failure Classification [D, S]**	**Failure rate origin**	**Failure rate [1/h]**	**No. 1**	**No. 2**	**No. 3**	**No. 4**
1	light source fault	D	manufacturer specificat.	1.2×10^{-7}				x
2	sample pressure high	D	operational experience	5.8×10^{-4}				
3	chiller fault	D	operational experience	1.2×10^{-4}			x	
4	sample flow low	D	operational experience	2.3×10^{-6}		x		
5	sample flow down	D	operational experience	2.3×10^{-7}	x			
6								
7								
8								
9								
10								

1) The effect on functional safety of PAT channel is not mentioned in this example

IEC

Figure B.1 – FMEDA – documentation of safety assessment (example)