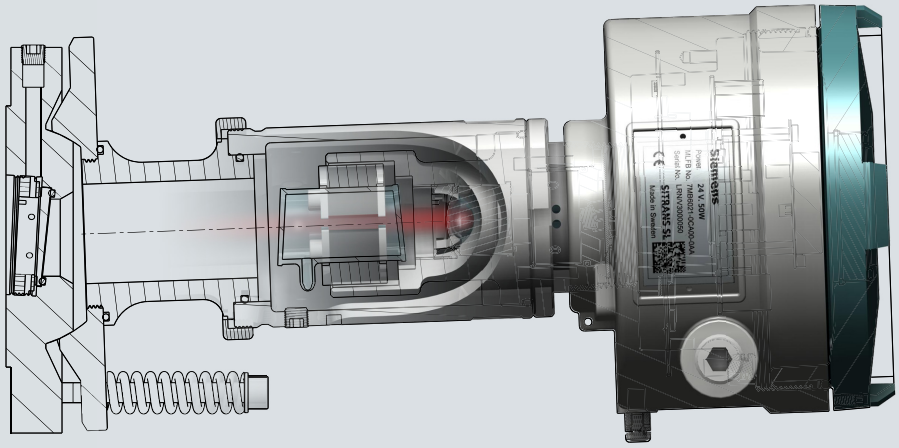
SITRANS SL

In-situ Laser Gas Analyzer

Safety Manual

Supplement to Operating Instructions



Continuous Gas Analysis

SIEMENS

SIEMENS

Continuous Gas Analysis

In-situ Laser Gas Analyzers Safety Manual

Operating Instructions

Supplement to SITRANS SL Operating Instructions

06/2012
A5E03433511-05

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE

indicates that an unintended result or situation can occur if the relevant information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

Order number: A5E03433511
℗ 06/2012 Technical data subject to change

Table of contents

Introduction

1

1.1 Purpose of this document

This document contains all information and safety instructions required when using the SITRANS SL in-situ gas analyzer in safety-instrumented systems.

It addresses system planners, constructors, service and maintenance engineers and any personnel commissioning and operating the device.

1.2 Device description

SITRANS SL is a gas analyzer employing single line molecular absorption spectroscopy. A diode laser emits a beam of infrared light which passes through the process gas and is detected by a receiver unit. The wavelength of the laser diode output is tuned to a gas specific absorption line. The laser continuously scans this single absorption line with a very high spectral resolution. The degree of absorption and the line shape are used for the evaluation. The measurement is free of cross-interferences, since the quasi-monochromatic laser light is absorbed very selectively by only one specific line in the scanned spectral range.

The field design of the SITRANS SL in-situ gas analyzer consists of a transmitter unit and a receiver unit. The light which is not absorbed by the sample is detected in the receiver. The concentration of the gas component is determined from the absorption.

The individual dependencies of concentration, pressure and temperature are application specific.

An internal reference cell is used to constantly check the stability of the spectrometer, thus assuring a continuous self-calibration of the analyzer.

The self-calibration of the analyzer is therefore valid for the time period specified in the technical data without the necessity for external recalibration using calibration gases.

1.3 Device variants

The following table lists all available SITRANS SL gas analyzer 4 to 20 mA variants, which meet the specific safety requirements of IEC 61508 / IEC 61511:

Product number (MLFB)	Measured component	SIL level	Assessment type
7MB6221-xAx0x-xxxx	Oxygen (O2)	SIL 1	IEC 61508 / IEC 61511 FMEDA incl. proven-in-use
7MB6221-xJx0x-xxxx	Carbon monoxide (CO)	SIL 1	IEC 61508 Hardware assessment (FMEDA)

The term SITRANS SL is used in the following text for all above-mentioned devices.

1.4 Additional documentation

This document deals with the SITRANS SL in-situ laser gas analyzer exclusively as part of a safety function. This document is valid only in conjunction with one of the following documents:

No.	Designation	Order no.
/1/	SITRANS SL Operating Instructions	A5E01132948 (English) A5E01132949 (German) A5E01132951 (French) A5E01132952 (Italian) A5E01132953 (Spanish)

1.5 History

The following table shows the released versions and the changes in the documentation compared to each preceding edition:

Edition	Remark
01 02/2011	First edition
02 06/2011	Introduction of CO as new measuring component
03 08/2011	Update of Certificate of Conformity
04 10/2011	Recalculation of safety function tolerance
05 06/2012	Proven in use for SITRANS SL O_2

1.6 Further information

Information

The contents of these instructions shall not become part of or modify any prior or existing agreement, commitment or legal relationship. All obligations on the part of Siemens AG are contained in the respective sales contract which also contains the complete and solely applicable warranty conditions. Any statements contained herein do not create new warranties or modify the existing warranty.

The content reflects the technical status at the time of printing. We reserve the right for technical changes in the course of further development.

References

If further information on an aspect described here is referenced to, the corresponding reference will always be found at the end of a section under "See also".

General description of functional safety

2

2.1 Safety-instrumented system

This chapter describes the functional safety in general and not specific to a device. The devices in the examples are selected as representative examples.

System description

The sensor (analyzer), logic unit/control system and final controlling element combine to form a safety-instrumented system, which executes a safety function.

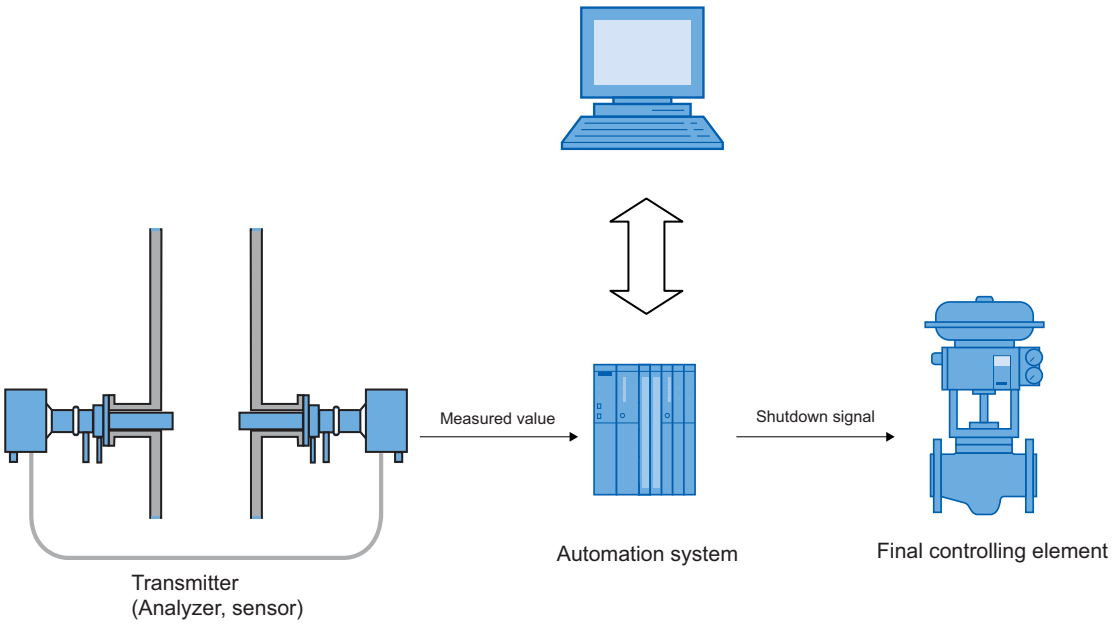


Figure 2-1 Safety-related system

Functional principle

The transmitter generates a process-related measured value that is transferred to the automation system. The automation system monitors this measured value. If the measured value exceeds the range of the high or low limit, the automation system generates a shutdown signal for the connected final controlling element, which switches the associated valve to the specified safety position.

2.2 Safety integrity level

Definitions

SIL, Safety Integrity Level

The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL) from SIL 1 to SIL 4. Each level corresponds to the probability range for the failure of a safety function. The higher the SIL of the safety-instrumented system, the higher probability that the required safety function will work.

The achievable SIL is determined by the following safety characteristics:

- Average probability of dangerous failure of a safety function in case of demand (PFD_{AVG})
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF)

Description

The following table shows the dependency of the SIL on the average probability of dangerous failures of a safety function of the entire safety-instrumented system" (PFD_{AVG}) The table deals with "Low demand mode", i.e. the safety function is required a maximum of once per year on average.

Table 2- 1 Safety Integrity Level

SIL	Interval
4	$10^{-5} \leq PFD_{AVG} < 10^{-4}$
3	$10^{-4} \leq PFD_{AVG} < 10^{-3}$
2	$10^{-3} \leq PFD_{AVG} < 10^{-2}$
1	$10^{-2} \leq PFD_{AVG} < 10^{-1}$

The "average probability of dangerous failures of the entire safety-instrumented system" (PFD_{AVG}) is normally split between the three sub-systems in the following figure.

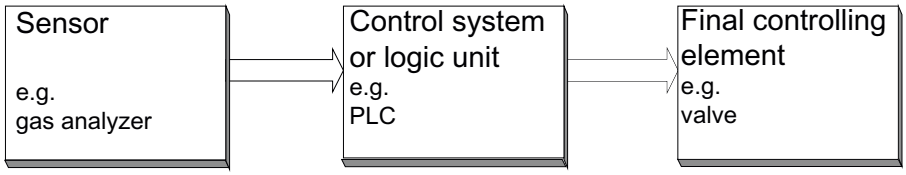


Figure 2-2 PFD distribution

The following table shows the achievable Safety Integrity Level (SIL) for the entire safety-instrumented system for type B subsystems depending on the proportion of safe failures (SFF) and the hardware fault tolerance (HFT). Type B subsystems include sensors with positioners, actuators with complex components, e.g. microprocessors (see also IEC 61508, Section 2).

Table 2- 2 Achievable Safety Integrity Level (type B subsystems)

SFF	HFT		
	0	1 (0) *	2 (1) *
< 60 %	Not allowed	SIL 1	SIL 2
60 ... 90 %	SIL 1	SIL 2	SIL 3
90 ... 99 %	SIL 2	SIL 3	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4

* As per IEC 61511-1, Section 11.4.4

Operational reliability

According to IEC 61511-1, Section 11.4.4, the hardware fault tolerance (HFT) can be reduced by one (values in brackets) for transmitters and final controlling elements with complex components if the following conditions are applicable to the device:

- The device is proven in operation.
- The user can configure only the process-related parameters, e.g. control range, signal direction in case of a fault, limiting values, etc.
- The configuration level of the firmware is blocked against unauthorized operation.
- The function requires SIL of less than 4.

The device fullfils these conditions.

Device-specific Safety Instructions 3

3.1 Applications

The SITRANS SL is suitable for use in a safety-instrumented function of Safety Integrity Level (SIL) 1, low demand mode, within a 1oo1 architecture.

The safety-related characteristics listed in the respective "SIL Declaration of Conformity" may be used in the relevant calculations required for IEC 61508 / 61511 safety-instrumented system compliance.

3.2 Safety function

The safety function at SITRANS SL refers to the measurement of gas concentrations.

The concentration is converted into an analog measured value and supplied over a 4 ... 20 mA (NAMUR) analog output. Fault tolerance allowances must be made, because the measured value transferred to the automation system by SITRANS SL can deviate from the physical value. The total tolerance (safety function) is calculated as follows:

Total tolerance (safety function) = ± [application-specific measuring error at operating conditions + 5 % safety accuracy of full-scale value].

The application-specific measuring error at operating conditions is calculated from the application-specific measuring error under reference conditions and the measuring error caused by the influencing variables which depend on the operating conditions. The application-specific measuring error under reference condition is 2 % of the full-scale value.

For the calculation of the measuring error of the influencing variables and external sensors contact SIEMENS support providing the operating conditions of the measurement point.

Safety accuracy of the SITRANS SL: the maximum effect of a single failure on the measured value, which is classified to have no effect.

The diagnostics function responds within 10 seconds in the worst-case scenario.

⚠ WARNING

The mandatory settings and conditions are listed in the "Settings (Page 16)" and "Safety characteristics (Page 20)" sections.

These conditions must be adhered to in order to fulfill the safety function.

The system component is of type B. For detailed information on values and hardware/firmware versions, refer to the manufacturer declaration for the product (Declaration of Conformity, Functional Safety according to IEC 61508 and IEC 61511).

The combination of sensor, automation system and final controlling element forms a safety-related system that performs a safety function. The emphasis of this description is on the sensor. For information on requirements for the automation system or final controlling element, refer to the corresponding standards and the extended list of proof tests in Maintenance and checks (Page 18).

If the device detects a failure (by diagnosis), the system must be brought to a safe state, and the device shall be repaired within the Mean Time To Restoration (MTTR).

The base of this PFD calculation is a MTTR of 72 hours.

See also

Certificate of Conformity SITRANS SL Functional Safety (http://support.automation.siemens.com/WW/view/en/10806991/134200)

3.3 Application restrictions

Installation and configuration of the SITRANS SL must be completed following the instructions detailed in the Operating Instructions of the device /1/. All application limitations and restrictions described in that manual must be observed.

3.3.1 Temperature and pressure

Safety recommendations for process temperature and process pressure

Process temperature and process pressure measurements have an influence on the concentration measurement by SITRANS SL and thus must be considered upon installation of the analyzer. The measurement of temperature and pressure must reflect the process conditions at the measurement point. Otherwise the error in concentration measurement increases.

If the process conditions for temperature and pressure can not assumed to be constant, external sensors for temperature and pressure are highly recommended. SITRANS SL provides two analog input channels (4 to 20 mA) for external temperature and pressure signals. Any external sensor for temperature and pressure must meet the requirements for SIL 1 with a maximum total tolerance (safety function) of ±5 %.

To calculate the error in the concentration measurement which is caused by an error of process temperature and/or process pressure measurement contact SIEMENS support providing the operating conditions of the measurement point and the total tolerance (safety function) of the external sensors.

3.3.2 Purging

Safety Recommendations for Purging

Purging of sensors is always required for applications with oxygen as gas to be measured. In this case the sensors require continuous purging using nitrogen. For detailed information, refer to respective chapters in the user manual.

Upon installation of the analyzer the use of an external monitoring system must be considered. This system must be designed to constantly monitor the purging flow and to ensure that all possible faults are signalled to the Safety PLC.

3.4 Settings

After assembly and commissioning in line with the device manual, the following parameter settings shall be made when the devices is used as part of a SIF:

Safety parameters

Enter the following parameter via SITRANS SL LUI setup menu:

Function	Action
Temperature correction	Set source for temperature compensation
Pressure correction	Set source for pressure compensation
Output configuration	Select analog output 0 for gas component
Path length	Enter correct path length

Enter the following parameter via configuration tool LDSComm:

Function	Action
Alarm configuration*	Select System I/O / Analog Outputs / Analog Output 0 tab. Set alarm action for all faults and warnings to 3 mA.

*Performing this configuration requires LDSComm user level "service".

References

- SITRANS SL Operating instructions /1/
- LDSComm Operating manual (Article no. A5E02350886)

Protection against configuration changes

After configuration, the SITRANS SL LUI password shall be changed using the LDSComm software to protect the device against unintentional and unauthorized changes/operation. Within LDSComm the LUI password can be found under the Device/Service tab. This entry requires LDSComm user level "service".

Checking the safety function after installation

Following installation and commissioning of the SITRANS SL a safety function test has to be carried out as described in section Maintenance and checks (Page 18) .

3.5 Behavior in case of faults

Faults

The procedure in case of faults is described in the Operating Instructions of the device.

Repairs

Defective devices should be sent to the Repair Department stating details and cause of any fault. When ordering replacement devices, also the serial number of the original device shall be mentioned. The serial number can be found on the nameplate.

Reference

Addresses of the responsible repair center, contact partners, spare parts lists etc. can be obtained from the SITRANS SL Operating instructions, sections A.4 and A.5 as well as from the following web address:

See also

web (http://support.automation.siemens.com)

3.6 Maintenance and checks

Checking the analyzer functions

We strongly recommend to check the function capability of the SITRANS SL at regular intervals. This can be achieved by use of the verification kit.

Details of the verification procedure, the equipment and the time intervals are described in the operating instructions, chapters 9 and 11.

Functional safety proof test

You should regularly check the safety function of the entire safety circuit according to IEC 61508/61511.

The test interval is determined during calculation of each individual safety circuit in a system (PFD_{AVG}). The recommended testing interval depends largely on the application but should not exceed one year.

To detect dangerous faults the SITRANS SL analog output and analog input shall be checked with the following tests.

Table 3- 1 Proof test part 1

Step	Action
1	Bypass the safety PLC or take another appropriate action to avoid a false trip.
2	Generate or simulate an alarm condition to force the SITRANS SL analyzer to exceed the low alarm current output limit and verify the analog current value (e.g. by disconnecting pressure / temperature input).
3	Restore the loop to full operation.
4	Remove the bypass from the safety PLC and restore to normal operation.

Table 3- 2 Proof test part 2

Step	Action
1	Bypass the safety PLC or take another appropriate action to avoid a false trip.
2	Carry out an instrument verification according to section 9.1 of the operating instructions /1/.
3	Restore the loop to full operation.
4	Remove the bypass from the safety PLC and restore to normal operation.

Table 3- 3 Proof test part 3 (only required if external sensors are used)

Step	Action
1	Bypass the safety PLC or take another appropriate action to avoid a false trip.
2	Select analog input test for Analog Temperature using LUI (local user interface).
3	Connect a calibrated current source, e.g. a loop calibrator, to the analog input 0 for temperature. Note: the current measuring instrument used for this test shall provide an accuracy of 0.1 % or better.
4	Apply at least the following currents in succession: 4.0 mA, 20.0 mA, and a current value within this interval to the analog input. The indicated measured values [mA] shall not deviate more than 0.5 % from the applied current.
5	Select analog input test for Analog Pressure using LUI.
6	Connect a calibrated current source, e.g. a loop calibrator to the analog input 1 for pressure. Note: the current measuring instrument used for this test shall provide an accuracy of 0.1 % or better.
7	Apply at least the following currents in succession: 4.0 mA, 20.0 mA, and a current value within this interval to the analog input. The indicated measured values [mA] shall not deviate more than 0.5 % from the applied current.
8	Restore the loop to full operation.
9	Remove the bypass from the safety PLC and restore to normal operation.

Table 3- 4 Proof test part 4

Step	Action
1	Bypass the safety PLC or take another appropriate action to avoid a false trip.
2	Unlock the LUI using the service password (Security menu).
3	Select analog output test / analog output 0 using LUI.
4	Connect a calibrated current measuring instrument with loop powering capability, e.g. a loop calibrator, to the analog output 0. Note: the current measuring instrument used for this test shall provide an accuracy of 0.1 % or better.
5	Set at least the following currents in succession: 4.0 mA, 20.0 mA, and a current value within this interval to the analog output. The measured current shall not deviate more than 0.5 % from the set current.
6	Select analog output test / analog output 1 using LUI.
7	Connect a calibrated current measuring instrument with loop powering capability, e.g. a loop calibrator, to the analog output 1. Note: the current measuring instrument used for this test shall provide an accuracy of 0.1 % or better.
8	Set at least the following currents in succession: 4.0 mA, 20.0 mA, and a current value within this interval to the analog output. The measured current shall not deviate more than 0.5 % from the set current.
9	Restore the loop to full operation.
10	Remove the bypass from the safety PLC and restore to normal operation.

3.7 Safety characteristics

The safety characteristics necessary for use of the system are listed in the SIL declaration of conformity. These values apply under the following conditions:

- The SITRANS SL is only used in safety-related systems with a low demand mode for the safety function
- When external sensors for process temperature and process pressure are used they have to be considered as part of the Safety related system.
- Purging of sensors must be considered as part of the Safety related system.
- The safety-related parameters/settings (see chapter Settings (Page 16)) have been entered by local operation and checked before starting safety-instrumented operation.
- The SITRANS SL is blocked against unintentional and unauthorized changes/operation.
- All used materials are compatible with process conditions.
- The MTTR after a device fault is 72 hours.
- The logic solver (PLC) has to be configured to detect low range (<3.6 mA) failure of the SITRANS SL (fail low) and will recognize these as internal failure of the devices and not cause a spurious trip.

See also

Certificate of Conformity SITRANS SL Functional Safety
(http://support.automation.siemens.com/WW/view/en/10806991/134200)

List of abbreviations 4

Abbreviations

Abbreviation	Full term	Meaning
>	Greater than	Mathematical sign for inequality
<	Less than	Mathematical sign for inequality
%	Percent	Mathematical sign for the hundredth part of a whole
CO	Carbon monixide or carbonous oxide (molecular formula)	A colorless, odorless, and tasteless gas, which is highly toxic to humans and animals in higher quantities. It consists of one carbon atom and one oxygen atom, connected by a triple bond that consists of two covalent bonds as well as one dative covalent bond. In case of SITRANS SL: A measuring component
DC	**D**iagnostic **C**overage	Parameter which describes the ratio of the failure rate of detected dangerous failures to the failure rate of all dangerous failures.
FIT	**F**ailure **I**n **T**ime	Frequency of failures of the protective function.
FMEDA	**F**ailure **M**odes, **E**ffects and **D**iagnostic Coverage **A**nalysis	Method to determine out of an overall failure rate of a system the proportion of failures without the potential to bring the safety-instrumented system into a dangerous or impermissible functional status (SFF) and the diagnostic coverage (DC) according to the requirements to IEC 61508.
HFT	**H**ardware **F**ault **T**olerance	Capability of a function unit to continue execution of a required function in the presence of faults or deviations.
IEC	**I**nternational **E**lectrotechnical **C**ommission	An international standards organization dealing with electrical, electronic and related technologies
I/O	**I**nput/**O**utput	I/O refers to the communication between an information processing system (such as a computer), and the outside world, such as a human, or another information processing system. Inputs are the signals or data received by the system, and outputs are the signals or data sent from it.
LUI	**L**ocal **U**ser **I**nterface	User interface for access to Siemens Process analyzers and instruments
mA	**M**illiampere	A unit of electrical current
MLFB	**M**aschinenlesbare **F**abrikate**b**ezeichnung	German for Machine-readable product identification, a product code
MTBF	**M**ean **T**ime **B**etween **F**ailures	Average period between two failures
MTTR	**M**ean **T**ime **T**o **R**epair	Average period between the occurrence of a fault on a device or system and its repair
NAMUR	**N**ormen**a**rbeitsgemeinschaft für **M**ess- **u**nd **R**egeltechnik	NAMUR is an international user association of automation technology in process industries

Abbreviation	Full term	Meaning
O_2	**O**xygen (molecular formula)	Chemical element with atomic number 8 and represented by the symbol O. Its name derives from the Greek roots ὀξύς (acid, literally "sharp", referring to the sour taste of acids) and -γενής (producer, literally begetter), because at the time of naming, it was mistakenly thought that all acids required oxygen in their composition. At standard temperature and pressure, two atoms of the element bind to form dioxygen, a colorless, odorless, tasteless diatomic gas with the formula O_2. In case of SITRANS SL: A measuring component
PFD	**P**robability of **F**ailure on **D**emand	Probability of dangerous failures of a safety function on demand
PFD_{AVG}	**P**robability of **F**ailure on **D**emand (**AV**ERA**G**E)	Average probability of dangerous failures of a safety function on demand
PLC	**P**rogrammable **L**ogic **C**ontroller	A digital computer used for automation of industrial processes, such as machinery control in factories
SFF	**S**afe **F**ailure **F**raction	Proportion of safe failures: Proportion of failures without the potential to bring the safety-instrumented system into a dangerous or impermissible functional status.
SIF	**S**afety **I**nstrumented **F**unction	Function to be implemented by a safety-related system or an external risk reduction facility, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event
SIL	**S**afety **I**ntegrity **L**evel	The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a probability range for failures of a safety function. The higher the Safety Integrity Level of the safety-instrumented system, the lower the probability that it will not execute the required safety functions.
TI	**T**est **I**nterval	Testing interval of the protective function
XooY	**X** **o**ut **o**f **Y** voting	Classification and description of the safety-instrumented system in terms of redundancy and the selection procedures used in which - Y specifies how often a safety function is executed (redundancy) and - X determines how many channels have to work correctly. Example: Pressure measurement in a 1oo2 architecture: A safety instrumented-system decides that a specified pressure limit has been exceeded if one out of two pressure sensors reaches this limit. In a 1oo1 architecture, there is only one pressure sensor.

Glossary

Dangerous failure

Failure with the potential to bring the safety-instrumented system into a dangerous or non-functional status

Fail-safe

The capability of a control to maintain the safe state of the controlled device, e.g. machine, process, or to bring the device to a safe state even when faults/failures occur.

Failure/Fault

Failure:
A resource is no longer capable of executing a required function.

Fault:
Undesired state of a resource indicated by the incapability of executing a required function.

Fault tolerance

Fault tolerance n means that a device can execute the intended task even when n faults exist. The device fails to execute the intended function in case of n+1 faults.

Final controlling element

Converter that converts electrical signals into mechanical or other non-electrical variables.

Low Demand Mode

The frequency of demands for operation made on a safety-related system is not more than one per year and not more than twice the proof-test frequency.

Risk

The combination of the probability of a damage occurring and its magnitude.

Safety function

Defined function executed by a safety-instrumented system with the objective of achieving or maintaining a safe system status which takes into account a defined occurrence of dangerous failures.

Example:
Monitoring of user-defined limit values.

Safety-instrumented system

A safety-instrumented system excludes the safety functions that are required to achieve or maintain a safe status in a system. It consists of a sensor, a logic unit/control system and a final controlling element.

Example:
A safety-instrumented system is made up of an analyzer (e.g. to measure an O_2 concentration), a PLC and a control valve.

Sensor

Converter that converts mechanical or other non-electrical variables into electrical signals.

Siemens AG
Industry Sector
Sensors and Communication

76181 KARLSRUHE
GERMANY

Subject to changes without prior notice
ID: A5E03433511

www.siemens.com/processanalytics