Functional Safety Manual · June 2009

million
in one

pointek

CLS500/LC500

SIEMENS

SIEMENS

Level Switch
Pointek CLS500
SITRANS LC500

SIL Safety Manual

Introduction 1

General safety instructions 2

Device-specific safety instructions 3

Appendix A

List of abbreviations / acronyms B

Pointek CLS500 series:
7ML5601*-Z C20, 7ML5602*-Z C20,
7ML5603*-Z C20, 7ML5604*-Z C20

SITRANS LC500
7ML5513*-Z C20, 7ML5515*-Z C20, 7ML5517*-Z C20,
7ML5521*-Z C20, 7ML5523*-Z C20

06/2009

Safety Guidelines

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 corresponding 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 device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

Warning

This device may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

All names identified by ® are registered trademarks of the 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.

Siemens AG
Automation and Drives
Postfach 4848, 90327 Nuremberg, Germany

Siemens Aktiengesellschaft

A5E00442122-01

Table of contents

1 Introduction 4
1.1 Purpose of this document 4
1.2 Required documentation 4
1.3 History 4
1.4 More information 5
2 General safety instructions 6
2.1 Safety-instrumented system 6
2.2 Safety Integrity Level (SIL) 9
3 Device-specific safety instructions 11
3.1 Applications 11
3.2 Safety function 11
3.3 Settings 12
3.4 Behavior in case of faults 13
3.5 Maintenance / Checking 13
3.6 Safety characteristics 14
A Appendix 15
A.1 SIL Declaration of Conformity 15
A.2 Exida Test Report (extract) 16
B List of abbreviations/acronyms 18
B.1 Abbreviations 18
Glossary 19

1

1 Introduction

1.1 Purpose of this document

This document deals with the Pointek CLS500 Level Switch and SITRANS LC Level Meter exclusively as part of a safety function.

It is aimed at system planners, constructors, service and maintenance engineers and personnel who will commission the device.

1.2 Required documentation

This document deals with the Pointek CLS 500 Level Switch and SITRANS LC500 Level Meter exclusively as part of a safety function. This document only applies in conjunction with the following documentation:

No.	Name	Order No.
/1/	Pointek CLS500 INSTRUCTION MANUAL	7ML19985GG01
/2/	SITRANS LC500 INSTRUCTION MANUAL	7ML19985GE01

1.3 History

The most important changes in the documentation when compared with the respective previous edition are given in the following table:

Edition	Comment
01 10/2005	First edition Safety manual order #: 7ML19985KK01
02 06/2009	Clarification of product numbering for product versions covered by SIL declaration of conformity • Sections: 1.1 • Appendices: A.1

1.4 More 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 to make technical changes in the course of further development.

References

If there are references to further information on an aspect described here, these will always be found at the end of a chapter under “See also”.

Siemens regional offices

If you need more information or have particular problems which are not covered sufficiently by the operating instructions, contact your local Siemens Regional Office. You will find the address of your local Siemens Regional Office on the Internet at https://www.siemens.com/processinstrumentation/contacts

Product information on the Internet

The Instruction Manual is on the supplied CD and is also available on the Siemens Level homepage on the Internet: www.siemens.com/level

On the supplied CD, you will also find the product catalog sheet containing the ordering data, the Device Install software for SIMATIC PDM for subsequent installation, and the generic station description (GSD).

See also

Siemens Regional Offices
(https://www.siemens.com/processinstrumentation/contacts)

Product information and Instruction Manuals on the Internet
(http://www.siemens.com/level)

2

2 General safety instructions

2.1 Safety-instrumented system

Definition: Safety-instrumented system

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

Example:

A safety-instrumented system is made up of a pressure transmitter, a logic unit and a control valve.

Definition: Safety function

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

Example:

Level switch for overflow protection

Definition: Dangerous failure

Failure with the potential to bring the safety-instrumented system into a dangerous on nonfunctional status.

Description

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

Notes

This document deals with the Pointek CLS500 and SITRANS LC500 exclusively as part of a safety function.
Pointek CLS500 and SITRANS LC500 devices covered by SIL declaration of conformity are identified by the “-Z C20” suffix of their product number which is printed on the device nameplate.

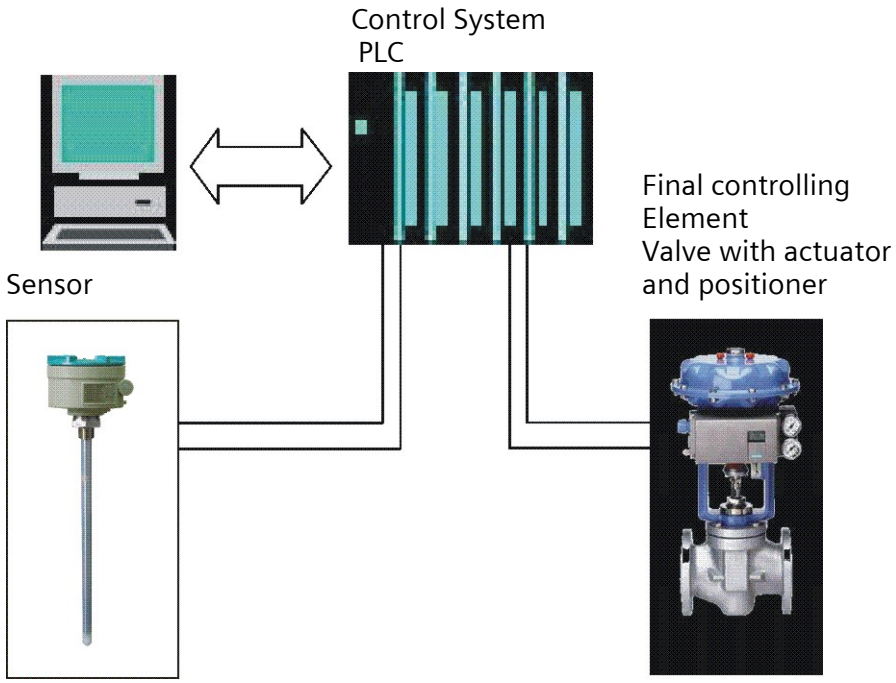

Figure 2-1 Example of a safety-instrumented system

Function

The SITRANS LC500 and Pointek CLS500 are capacitance instruments for level and interface measurements. They have a modular configuration of probe and 2-wire transmitter as one instrument. The integrated zener safety barrier blocks excess energy from the transmitter to the sensor for intrinsically safe conditions.

The SITRANS LC500 can be used with rod or cable probes and allows for probe versions up to 5.5 m (18 ft) for the rod version and up to 35 m (115 ft) for the cable version. The Pointek CLS500 can be used with rod type probes up to 1 m (3.3 ft) in length. The measurement is unaffected by moisture, vapors, foam, temperature and pressure variations, or material build-up around the mounting glands.

The SITRANS LC500 and Pointek CLS500 are two wire smart devices. For safety-instrumented systems usage it is assumed that the 4-20 mA output is used as the primary safety variable. In addition to the 4-20 mA output, a solid state switch relay output is available. For the Failure Modes, Effects and Diagnostic Analysis it was assumed that the relay output is used to signal diagnostic information (in addition to the current signaling according to NAMUR NE 43).

The following table gives an overview of the different versions that were considered in the FMEDA of the SITRANS LC500 and Pointek CLS500. This corresponds with type numbers: MSP2002-1 (330pF), MSP2002-2 (3300 pF), and MSP2002-3 (6600pF).

SITRANS LC500	4-20/20-4mA signal & 2-state functionality 4 or 20/20 or 4 mA, on or off
Pointek CLS500	4-20/20-4mA signal & 2-state functionality 4 or 20/20 or 4 mA, on or off

2.2 Safety Integrity Level (SIL)

Definition: SIL

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 in 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.

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

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

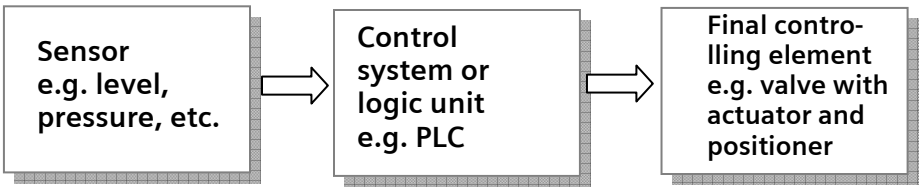

Figure 2-2 PFD_{AVG} distribution

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

SFF	HFT		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60 to 90%	SIL 1	SIL 2	SIL 3
90 to 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

3 Device-specific safety instructions

3.1 Applications

The Pointek CLS500 and the SITRANS LC500 satisfy the special requirements in terms of functional safety to SIL 1 in accordance with IEC 61508 or IEC 61511-1.
The Pointek and SITRANS are usable in safety applications in case of overfill or underfill protection.
These meet the following requirements:

- Functional safety according to SIL 1 under IEC 61508 or IEC 61511-1
- Electromagnetic compatibility in accordance with EN 61326/A1, Appendix A1.

3.2 Safety function

Safety function on Pointek CLS500 and SITRANS LC500. The safety function is the detection of high level alarms in case of overfill protection, or low level alarms in case of underfill protection.

The difference in capacitance between a covered probe and an uncovered probe (for example, between a probe in water and a probe in air), is used to detect level, and to protect the process from a level that is too high or too low.

The following table gives an overview of the different versions that were considered in the FMEDA of the SITRANS LC500 and Pointek CLS500. This corresponds with type numbers: MSP2002-1 (330pF), MSP2002-2 (3300 pF), and MSP2002-3 (6600pF).

SITRANS LC500	4-20/20-4mA signal & 2-state functionality 4 or 20/20 or 4 mA, on or off
Pointek CLS500	4-20/20-4mA signal & 2-state functionality 4 or 20/20 or 4 mA, on or off

As seen in the above table, the mA output can be used a continuous 4-20 mA (or 20-4 mA) signal, proportional to the surface level of the product, or as a 2-state switch set to either 4 or 20 mA. It can be set to go to 4 mA if the probe is covered and 20 mA if the probe is uncovered, or the reverse.

Warning

The binding settings and conditions are listed in the “Settings” and “Safety characteristics” sections. These conditions must be met in order to fulfill the safety function.

Reference

See chapter 1.2

See also

Settings (Chapter 3.3)
Safety characteristics (Chapter 3.6)

3.3 Settings

After assembly and commissioning in line with the device manual, the parameter settings should be made for the safety function as described in applicable reference /1/ or /2/.

Reference

Device manual

Protection against configuration changes

After configuration of the Pointek CLS500 or SITRANS LC500 you should fix the housing cover so that the device is protected against unwanted and unauthorized changes/operation.

Checking the safety function

After installation you shall test that the Pointek/SITRANS is switching correctly. First you shall test the basic functionality of the Pointek/SITRANS as described in device manual /1/ or /2/. To test the full safety case the sensor shall be covered. In this condition, the Pointek/SITRANS must switch to high level alarm (safety position).

3.4 Behavior in case of faults

Fault

The procedure in case of faults is described in the applicable device operating manual /1/ or /2/.

Repairs

Defective devices should be sent to the Repair Department with details of the fault and the cause. When ordering replacement devices, please specify the serial number of the original device. The serial number can be found on the nameplate.

The address of the responsible repair center, contact, spare parts lists etc. can be found on the Internet at:

Reference

www.siemens.com/automation/services&support
www.automation.siemens.com/partner

3.5 Maintenance / Checking

Checking function

We recommend that the functioning of the Pointek/SITRANS is checked at regular Intervals of one year.
Check at least the following:

- Test the basic functionality of the Pointek/SITRANS as described in Device manual /1/ or /2/

Checking safety

You should regularly check the safety function of the entire safety circuit in line with IEC 61508/61511.
The testing intervals are determined during circulation of each individual safety circuit in a system (PFD_{AVG}). Recommended proof test interval is 1 year.

On the Pointek/SITRANS Level Switch the following specific checks shall be carried out:

- Test the basic functionality of the Pointek/SITRANS as described in Device manual /1/ or /2/
- Test the full safety functionality by
  - Check the output state of Pointek/SITRANS if sensor is uncovered : not switched
  - Cover the sensor: Pointek CLS500, SITRANS LC500 must switch.

3.6 Safety characteristics

The safety characteristics necessary for use of the system are listed in the SIL declaration of conformity (see chapter A.1). These values apply under the following conditions:

- The Pointek CLS500; SITRANS LC500 is only used in applications with a low demand rate for the safety function (low demand mode).
- The safety-related parameters /settings (see Settings chapter 3.3) have been entered by local operation and checked before commencing safety-instrumented operation.
- The Pointek/SITRANS is blocked against unwanted and unauthorized changes/operation.
- The average temperature viewed over a long period is ≤ 40 °C.
- All used materials are compatible with process conditions.
- The MTTR after a device fault is 8 hours.
- The best time to react on a dangerous detected failure is 1 hour.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low features are detected regardless of the effect, safe or dangerous, on the safety function.
- The logic solver is configured to detect overrange (>21mA) and underrange (<3.6mA) failure of the SITRANS LC500 and Pointek CLS500 (Fail High and Fail Low) and will recognize these as internal failure of the devices and not cause a spurious trip.
- The solid state switch relay output is used to signal diagnostic information (in addition to the current signaling according to NAMUR NE 43)

See also

Settings (chapter 3.3)
SIL Declaration of Conformity (chapter A.1)

A

A Appendix

A.1 SIL Declaration of Conformity

SIEMENS

Industry

SIL Declaration of Conformity

Functional Safety according to IEC 61508 and IEC 61511

No. A5E02559296A - 02

Manufacturer:	Siemens Milltronics Process Instruments Inc.
Hersteller:	Division I IA SC
Address:	1954 Technology Drive, P.O. Box 4225; Peterborough, Ontario;
Anschrift:	K9J 7B1, Canada
Product description:	**Pointek CLS 500 Level Switch and SITRANS LC 500 Level Transmitter**
Produktbezeichnung	Type: CLS 500: 7ML5601*-Z C20, 7ML5602*-Z C20, 7ML5603*-Z C20, 7ML5604*-Z C20
	Type: LC 500: 7ML5513*-Z C20, 7ML5515*-Z C20, 7ML5517*-Z C20, 7ML5521*-Z C20, 7ML5523*-Z C20

We as manufacturer declare that the following failure rates for the above identified hardware may be used in the relevant calculations required for IEC 61508 / 61511 safety instrumented system (SIS) compliance. The hardware of the device is capable of overfill or underfill protection with an accuracy of 2% of full span for a safety instrumented function of Safety Integrity Level (SIL) 1. The appropriate SIL safety instructions of the provided Functional Safety Application Manual shall be observed. The assessment did not include the evaluation of systematic safety integrity (software and development process); however product revisions will be carried out by the manufacturer in accordance with IEC 61508.

The FMEDA was carried out by Siemens in accordance with IEC 61508 and the results were reviewed by exida GmbH.

Safety Related Characteristics	CLS500	LC500
Device Type	**B**	**B**
SIL Safety Integrity Level	**1**	**1**
HFT	**0**	**0**
PFD_{AVG}	$6.55*10^{-4}$	$6.55*10^{-4}$
SFF Safe Failure Fraction	**82 %**	**82 %**
λ_{SD} Safe detected Failure Rate	**0 FIT**	**0 FIT**
λ_{SU} Safe undetected Failure Rate	**363 FIT**	**363 FIT**
λ_{DD} Dangerous detected Failure Rate	**344 FIT**	**344 FIT**
λ_{DU} Dangerous undetected Failure Rate	**149 FIT**	**149 FIT**

These characteristics are valid for low demand mode of operation within a 1oo1 architecture. (Guidance to calculation see IEC 61508-6, annex B). The PFD_{AVG} value is valid under the assumption of Mean Time To Restoration MTTR = 8h and Proof Test Interval T1 = 8760h.

Peterborough, June 02, 2009

Siemens Milltronics Process Instruments Inc.

S. Woodward — 2/06/09

Steven Woodward, VP of Technology signature — Alan Browne, Sr. Director of Operations signature

Siemens Milltronics Process Instruments Inc. *Page 1 / 1*

1954 Technology Drive, P.O. Box 4225
Peterborough, Ontario
K9J 7B1 / Canada

Tel.: (705) 745-2431
Fax: (705) 741-0466
www.siemens.com/processautomation

A.2 Exida Test Report (extract)

* Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Sitrans LC 500 and Pointek CLS 500 capacitance level transmitters. A Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the Sitrans LC 500 and Pointek CLS 500 level transmitters, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Sitrans LC 500 and Pointek CLS 500 level transmitters are two wire smart devices. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. Table 1 gives an overview of the different versions that were considered for the Sitrans LC 500 and Pointek CLS 500 when performing the FMEDA. This corresponds with type numbers: MSP2002-1 (330 pF), MSP2002-2 (3300 pF), and MSP2002-3 (6600pF).

Table 1 Version overview

Sitrans LC 500	4-20/20-4mA signal & 2-state functionality 4 or 20/20 or 4 mA, on or off
Pointek CLS 500	4-20/20-4mA signal & 2-state functionality 4 or 20/20 or 4 mA, on or off

The Sitrans LC 500 and Pointek CLS 500 level transmitters are classified as Type B[1] devices according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the devices have a Safe Failure Fraction between 60 and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents).

The failure rates for the Sitrans LC 500 and Pointek CLS 500 level transmitters are listed in Table 2.

Table 2 Failure rates Sitrans LC 500 and Pointek CLS 500

Failure category		Failure rate (in FITs)			
		Sitrans LC 500		Pointek CLS 500	
Fail Dangerous Detected			344		344
	Fail detected (int. diag.)	216		216	
	Fail low (detected by the logic solver)	70		70	
	Fail High (detected by the logic solver)	58		58	
Fail Dangerous Undetected			149		149
No Effect			322		322
Annunciation Detected			23		23
Annunciation Undetected			18		18

Table 3 lists the failure rates for the Sitrans LC 500 and Pointek CLS 500 level transmitters according to IEC 61508.

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

* See front cover of this manual for current Product Numbers and Descriptions.

Table 3 Failure rates according to IEC 61508, Sitrans LC 500 and Pointek CLS 500

Failure Category	λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF
Sitrans LC 500	0 FIT	363 FIT	344 FIT	149 FIT	82.6%
Pointek CLS 500	0 FIT	363 FIT	344 FIT	149 FIT	82.6%

These failure rates are valid for the useful lifetime of the product; see Appendix A.

A user of the Sitrans LC 500 and Pointek CLS 500 capacitance level transmitters can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

B

B List of abbreviations/acronyms

B.1 Abbreviations

Abbreviation	Full term in English	Meaning
FIT	Failure in Time	Frequency of failure of the protective function
HFT	Hardware Fault Tolerance	Hardware fault tolerance: Capability of a function unit to continue executing a required function in the presence of faults or deviations.
MTBF	Mean Time Between Failures	Average period between two failures
MTTR	Mean Time To Restoration	Average period between the occurrence of a fault on a device or system and the repair
PFD	Probability of Failure on Demand	Probability of dangerous failures of a safety function on demand
PFD_{AVG}	Average Probability of Failure on Demand	Average probability of dangerous failures of a safety function on demand
PLC	Programmable Logic Controller	
SIL	Safety Integrity Level	The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for failure 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.
SFF	Safe Failure Function	Proportion of safe failures: Proportion of failures without the potential to bring the safety instrumented system into a dangerous on no permissible functional status.
TI	Test Interval	Testing interval of the protective function
XooY	"X out of Y" voting	Classification and description of the safety-instrumented system in terms of redundancy and the selection procedures used.
		"Y" -Specifies how often the safety function is executed (redundancy).
		"X" -Determines how many channels have to work correctly.
		Example: Pressure measurement: 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 nonfunctional status

Safety function

Defined function executed by a safety-instrumented system with the objective of achieving or maintaining a safe system status taking into account a defined dangerous occurrence.
Example:
Limit pressure monitoring

Safety Integrity Level

→ SIL

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, logic unit/control system and final controlling element.
Example:
A safety-instrumented system is made up of a pressure transmitter, a limit signal sensor and a control valve.

SIL

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 the 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)

www.siemens.com/level

Siemens Milltronics Process Instruments Inc.
1954 Technology Drive, P.O. Box 4225
Peterborough, ON, Canada K9J 7B1
Tel: (705) 745-2431 Fax: (705) 741-0466
Email: techpubs.smpi@siemens.com

7ML19985KK02
Printed in Canada

Rev. 2.0