Functional Safety Manual · October 2009

million
in one

pointek

CLS200/CLS300

SIEMENS

SIEMENS

Level Switch
Pointek CLS200 / CLS300
(standard version)

SIL Safety Manual

Supplement to device Instruction Manual

Pointek CLS200:
7ML5502*-Z C20, 7ML5504*-Z C20, 7ML5505*-Z C20, 7ML5630*-Z C20, 7ML5631*-Z C20, 7ML5632*-Z C20, 7ML5633*-Z C20, 7ML5634*-Z C20

Pointek CLS300:
7ML5506*-Z C20, 7ML5507*-Z C20, 7ML5508*-Z C20, 7ML5510*-Z C20, 7ML5650*-Z C20, 7ML5651*-Z C20, 7ML5652*-Z C20

10/2009

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

1 Introduction

1.1 Purpose of this document

This document contains information and safety instructions that you will require when using the Pointek Level Switch in safety-instrumented systems.

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

1.2 Required documentation

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

No.	Name	Order No.
/1/	Pointek CLS200/CLS300 INSTRUCTION MANUAL	7ML19985JH01

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
1.0 10/2005	First edition Safety manual order #: 7ML19985KJ01
1.1 04/2007	Second edition to SMPI standards
2.0 06/2009	Clarification of product numbering for product versions covered by SIL declaration of conformity • Sections: 2.1 • Appendices: A.1
3.0 10/2009	Clarification of product numbering for product versions covered by SIL declaration of conformity • Sections: 1.2 • 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.

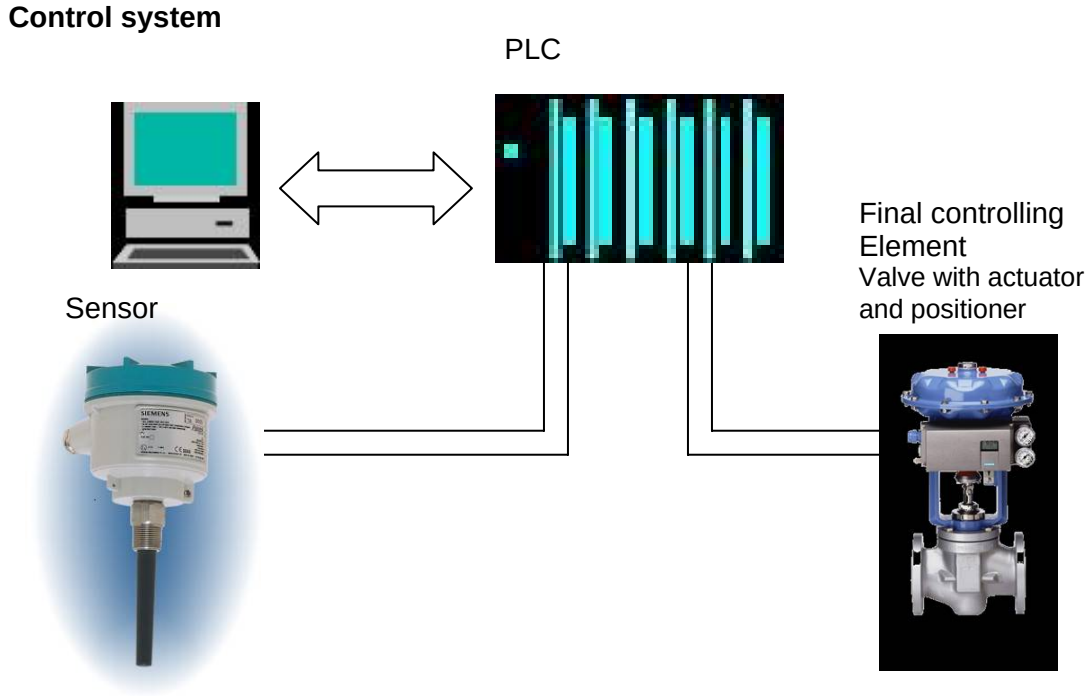

Figure 2-1 Example of a safety-instrumented system

Example:

A safety-instrumented system is made up of a level switch, 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 and final controlling element combine to form a safety-instrumented system, which executes a safety function.

Notes

This document deals with the Pointek CLS200/300 Standard versions exclusively as part of a safety function.
CLS200/300 devices covered by SIL declaration of conformity are identified by the “-Z C20” suffix to their product number which is printed on the device nameplate.

Function

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. The output switches (relay and interlinked solid-state switch), when the change in capacitance is greater than the setting at the trip point. This causes the control system to bring the process to a safe state.

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.

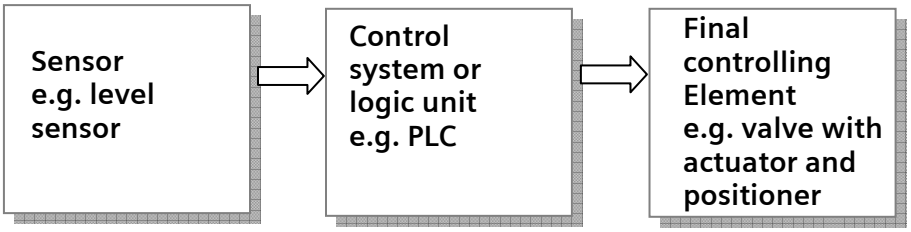

Figure 2-2 PFD_{AVG} distribution

The following table shows the achievable Safety Integrity Level (SIL) for the entire safety-instrumented system for type A systems depending on the proportion of safe failures (SFF) and the hardware fault tolerance (HFT). Type A systems include sensors and positioners without complex components, e.g. microprocessors (see also IEC 61508, Section 2).

SFF	HFT		
	0	1	2
<60%	SIL1	SIL2	SIL3
60 to 90%	SIL2	SIL3	SIL4
90 to 99%	SIL3	SIL4	SIL4
>99%	SIL4	SIL4	SIL4

3 Device-specific safety instructions

3.1 Applications

The Pointek Level Switches CLS200/300 standard versions satisfy the special requirements in terms of functional safety to SIL 2 in accordance with IEC 61508 or IEC 61511-1.
The Pointeks are usable in safety applications in case of overflow protection. These meet the following requirements:

- Functional safety according to SIL 2 under IEC 61508 or IEC 61511-1
- Electromagnetic compatibility in accordance with EN 61326/A1, Appendix A1.

3.2 Safety function

The Safety function on Pointek CLS200/300 standard version is the detection of high level alarms for overfill 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. The output switches (relay and interlinked solid state switch) when the change in capacitance is greater than the setting at the trip point. This causes the control system to bring the process into a safety state.

The trip point is set by potentiometer P2. This determines how large the difference in capacitance needs to be before the output is switched.

The safety function is overfill protection and can be detected by the following:

- Relay is De-energized
- Red LED is Off
- Solid-state switch is Open
- Alarm state in On

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 following parameter settings should be made for the safety function:

Safety parameters

S1-ON	Delay disabled	
S2-ON	Delay disabled	
S3-ON	High alarm	probe covered = alarm ON/relay de-energized
S4-OFF	Test function disabled	normal operation
S5-ON	High sensitivity	default setting for dry solids or non-conductive liquids

Reference

Device Instruction Manual

Protection against configuration changes

After configuration, fix the housing cover on the Pointek CLS200/300 so that the device is protected against unwanted and unauthorized changes/operation.

Checking the safety function

After installation you must test that the Pointek is switching correctly.

1. Test the basic functionality of the Pointek as described in Instruction Manual.
2. To test the full safety case, the sensor must be covered. In this condition, the Pointek 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 device operating manual /1/.

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 is checked at regular Intervals of one year.
Check at least the following:

- Test the basic functionality of the Pointek as described in Device Instruction Manual /1/.

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 Level Switch the following specific checks shall be carried out:

- Test the basic functionality of the Pointek as described in Device manual /1/.
- Test the full safety functionality:
    - Check the output state of Pointek if sensor is uncovered: not switched
    - Cover the sensor: Pointek CLS200 /300 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 CLS200/300 standard is only used for overfill protection in safety related applications.
- The Pointek CLS200/300 standard 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 is blocked against unwanted and unauthorized changes/operation.
- The DIP switch shall be in safety position (see Settings chapter 3.3)
- The average temperature viewed over a long period is ≤ 40 °C.
- All used materials are compatible with process conditions.
- Using the Pointek correctly there are no known wear-out mechanisms. The maximum lifetime of the relay output is 150 000 switching cycles.
- The MTTR after a device fault is 8 hours.
- The test time to react on a dangerous detected failure is 1 hour.
- A dangerous failure of the Pointek is a failure where the safety position is not activated, (high level alarm). The output stays on while the sensor is covered.

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. A5E02559298A – 3

Manufacturer: *Hersteller:*	Siemens Milltronics Process Instruments Inc. Division I IA SC
Address: *Anschrift:*	1954 Technology Drive, P.O. Box 4225; Peterborough, Ontario; K9J 7B1, Canada
Product description: *Produktbezeichnung*	**Pointek CLS 200 / CLS 300 (standard versions) Level Switch** **Type: CLS 200:** 7ML5502*-Z C20, 7ML5504*-Z C20, 7ML5505*-Z C20, 7ML5630*-Z C20, 7ML5631*-Z C20, 7ML5632*-Z C20, 7ML5633*-Z C20, 7ML5634*-Z C20 **Type: CLS 300:** 7ML5506*-Z C20, 7ML5507*-Z C20, 7ML5508*-Z C20, 7ML5510*-Z C20, 7ML5650*-Z C20, 7ML5651*-Z C20, 7ML5652*-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 protection with an accuracy of 2% of full span for a safety instrumented function of Safety Integrity Level (SIL) 2. 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	CLS200	CLS300
Device Type	**A**	**A**
SIL Safety Integrity Level	**2**	**2**
HFT	**0**	**0**
PFD_{AVG}	$6.56*10^{-4}$	$8.62*10^{-4}$
SFF Safe Failure Fraction	**77 %**	**66 %**
λ_{SD} Safe detected Failure Rate	**107 FIT**	**28 FIT**
λ_{SU} Safe undetected Failure Rate	**413 FIT**	**348 FIT**
λ_{DD} Dangerous detected Failure Rate	**8 FIT**	**9 FIT**
λ_{DU} Dangerous undetected Failure Rate	**150 FIT**	**197 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, September 30, 2009

Siemens Milltronics Process Instruments Inc.

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 hardware assessment carried out on the Level transmitters Pointek CLS 200 and Pointek CLS 300.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500.

SIEMENS and *exida* together did a quantitative analysis of the mechanical parts of the Level transmitters Pointek CLS 200 and Pointek CLS 300 to calculate the mechanical failure rates using different failure rate databases ([N5], [N6], [N7] and *exida*'s experienced-based data compilation) for the different mechanical components (see [R1] and [R2]). The results of the quantitative analysis are included in the calculations described in sections 5.2 and 5.3.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part. For a SIL 2 application the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the level transmitters would then be 3,50E-03.

The Level transmitters Pointek CLS 200 and Pointek CLS 300 are considered to be Type A[1] components with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

The following tables show how the above stated requirements are fulfilled.

Table 1: Summary for Pointek CLS 200 analog model – IEC 61508 failure rates

λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF	DC_S [3]	DC_D [3]
107 FIT	413 FIT	8 FIT	150 FIT	77%	20%	5%

Table 2: Summary for Pointek CLS 200 analog model – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 6,56E-04	PFD_{AVG} = 3,27E-03	PFD_{AVG} = 6,53E-03

[1] Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

[2] Note that the SU category includes failures that do not cause a spurious trip

[3] DC means the diagnostic coverage (safe or dangerous).

* See front cover of this manual for current Product Numbers and Descriptions. Any mention of *analog model* in this test report refers to the *standard version* of the product.

* **Table 3: Summary for Pointek CLS 300 analog model – IEC 61508 failure rates**

λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF	DC_S [3]	DC_D [3]
28 FIT	348 FIT	9 FIT	197 FIT	66%	7%	4%

Table 4: Summary for Pointek CLS 300 analog model – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 8,62E-04	PFD_{AVG} = 4,30E-03	PFD_{AVG} = 8,57E-03

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in green ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in red ( ) mean that the calculated PFD_{AVG} values do not fulfill the requirements for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996.

The assessment has shown that the Level transmitters Pointek CLS 200 analog model and Pointek CLS 300 analog model have a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of more than 66%.

The failure rates listed above do not include failures resulting from incorrect use of the Level transmitters Pointek CLS 200 analog model and Pointek CLS 300 analog model, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the Level transmitters Pointek CLS 200 and Pointek CLS 300 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). A full table of failure rates is presented in sections 5.2 and 5.3 along with all assumptions.

It is important to realize that the “no effect” failures and the “annunciation” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the Level transmitters Pointek CLS 200 and Pointek CLS 300, which is estimated to be 10 years (see Appendix 3).

* Any mention of *analog model* in this test report refers to the *standard version* of the product.

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 or 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

7ML19985KJ03
Printed in Canada

Rev. 3.0