



million
in one

pointek

ULS200

SIEMENS

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.

Disclaimer of liability

While we have verified the contents of this manual for agreement with the hardware and software described, variations remain possible. Thus we cannot guarantee full agreement. The contents of this manual are regularly reviewed and corrections are included in subsequent editions. We welcome all suggestions for improvement.

Copyright © SIEMENS AG 2009
Subject to change without further notice

SIEMENS

SITRANS

Level Instruments

Functional Safety for Pointek ULS200

Product Information

<u>Introduction</u>	1
<u>General safety instructions</u>	2
<u>Device-specific safety instructions</u>	3
<u>Appendix</u>	A
<u>List of abbreviations / acronyms</u>	B

Pointek ULS200:

7ML1510-1**0*-Z C20

7ML1510-2**0*-Z C20

7ML1510-3**0*-Z C20

24 V DC, relay output

24 V DC, transistor output

100 to 230 V AC, relay output

Ordering Number: 7ML1510-####
07/2009

Table of contents

1	Introduction.....	2
1.1	General.....	2
1.2	Purpose of this document	2
1.3	Required documentation.....	2
1.4	History	3
1.5	More information.....	4
2	General safety instructions	5
2.1	Safety-instrumented system (SIS)	5
2.2	Safety Integrity Level (SIL).....	6
3	Device-specific safety instructions.....	8
3.1	Applications.....	8
3.2	Safety function	8
3.3	Application restrictions	9
3.4	Settings.....	9
3.5	Behavior in case of faults	10
3.6	Maintenance/Testing	11
3.7	Safety characteristics.....	12
A	Appendix	13
A.1	SIL Declaration of Conformity.....	13
A.2	FMEDA and Proven-in-use Report (extract).....	14
B	List of Abbreviations/Acronyms	16
B.1	Abbreviations	16
	Glossary.....	17

1

1 Introduction

1.1 General

The following table lists all available Pointek ULS200 models:

Power Supply / Output - Type	Product Number
24 V DC, relay output	7ML1510-1**0*
24 V DC, transistor output	7ML1510-2**0*
100 to 230 V AC, relay output	7ML1510-3**0*

ULS200 devices covered by SIL declaration of conformity are identified by the “-Z C20” suffix to their product number which is printed on the device name plate.

The term ULS200 is used in the following text for all device models.

1.2 Purpose of this document

This document contains information and safety instructions required when using the ULS200 in a safety-instrumented system.

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

1.3 Required documentation

This document deals with the “Point Level Measurement – Pointek ULS200” exclusively as part of a safety function. This document only applies in conjunction with the following documentation:

No.	Name	Order No.
/1/	Instruction Manual Pointek ULS200	7ML19981XB82: Multi language Quick Start Instruction Manual

* Instruction Manuals are located at the following web site:
<http://www.siemens.com/level>

1.4 History

This history establishes the correlation between the current documentation and the valid firmware of the device.

The documentation of this edition is applicable for the following firmware:

Edition	Firmware identification type plate
04/2007	FW: from V 9.10

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

Edition	Comment
01 04/2007	First edition Safety manual order #: 7ML19985KC01
02 07/2009	Clarification of product numbering for product versions covered by SIL declaration of conformity <ul style="list-style-type: none">• Sections: 1.1• Appendices: A.1

1.5 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.

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.

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 General safety instructions

2.1 Safety-instrumented system (SIS)

Description

An instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensors, logic solvers or control systems (PLCs), and final elements.

Control system

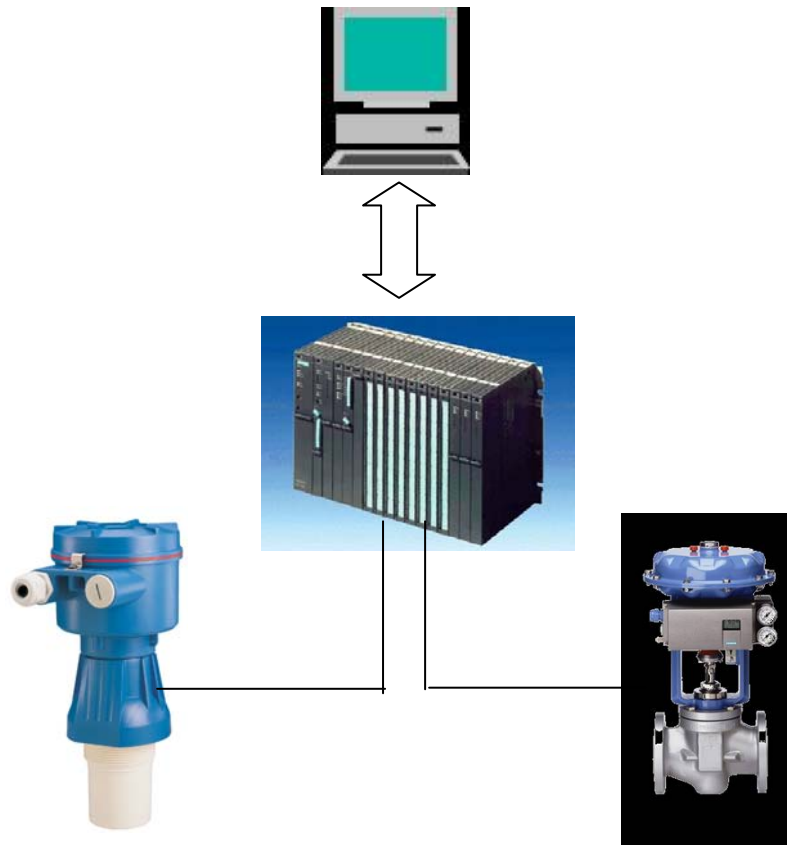


Figure 2-1: Example of a safety-instrumented system

Device Operation

Pointek ULS200 is an ultrasonic based process level switch providing overflow and dry run protection. The output switches activate an relay or transistor when the predefined threshold value is exceeded (overflow) or when the level falls below the predefined threshold value (dry run). Switching the output causes the control system to bring the process into 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 lower the probability that the required safety function will experience a dangerous failure.

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)
- Measures for Systematic Safety Integrity

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 to act a maximum of once per year on average.

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

The average probability of dangerous failures of the entire safety instrumented function (PFD_{AVG}) is calculated based on the three subsystems shown in the following figure.

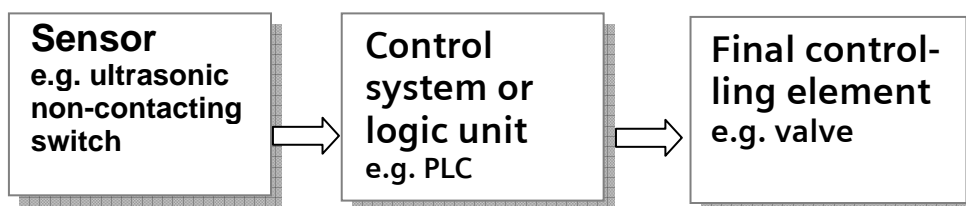


Figure 2-2: PFD_{AVG} distribution

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

SFF	HFT		
	0	1 (0) ¹⁾	2(1) ¹⁾
< 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

¹⁾ As per IEC 61511-1, Section 11.4.4

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

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

The ultrasonic switch fulfills these conditions.

3 Device-specific safety instructions

3.1 Applications

This hardware assessment of the Pointek ULS200 shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of systematic safety integrity (software and development process).

The hardware of ULS200 satisfies the hardware safety integrity requirements up to SIL 1 in accordance with IEC 61508 and IEC 61511-1.

3.2 Safety function

The output switches (relay / transistor) may be used as part of a safety instrumented function (SIF). A dangerous failure is defined as a deviation of the programmed switching level of $\pm 2\%$ of full span.



Warning

The settings and conditions listed in the “*Settings*” and “*Safety characteristics*” sections of this document must be met for the safety function specification to be valid.

If the device indicates a diagnostic failure, the system must be brought to a failsafe state, or the device shall be repaired within the Mean Time To Restoration (MTTR). The base of this PFD calculation is a MTTR of 8 hours.

The maximum operating lifetime of the ULS200 in a SIF is 10 years¹. After this time, the device must be replaced.

Reference

Pointek ULS200 Instruction manual (*Chapter 1.3*)

See also

Settings (*Chapter 3.4*)

Safety characteristics (*Chapter 3.7*)

¹ The operation temperature has a direct impact on this time. Therefore, a small deviation from the ambient operation temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows “The Doubling 10 °C Rule” where life is doubled for each 10 °C reduction in operating temperature.

3.3 Application restrictions

In case of minimum (MIN) detection, the following causes lead to the situation where the ultrasonic based process level switch Pointek ULS200 can no longer be used for safety related functions with the listed failure rates, Safe Failure Fraction and PFD_{AVG} :

- Thick and/or solid build-up
- False echoes from flat obstructions or obstructions with a sharp edge
- Applications using agitators
- Foam with a density $> 5 \text{ g/cm}^3$

In case of maximum (MAX) detection, the following causes lead to the situation where ultrasonic based process level switch Pointek ULS200 can no longer be used for safety related functions with the listed failure rates, Safe Failure Fraction, and PFD_{AVG} .

- Presence of a CO_2 blanket

3.4 Settings

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

Safety parameters

Please enter following parameters using the ULS200 menu:

For Overfill / High level protection:

Parameter	Comment
Fcn: Output Function	The Output Function shall be set to 4 (high alarm)
FLS: Fail-Safe Mode	The Fail-Safe Mode shall be set to 1 (high)
FSt: Fail-Safe Timer	The Fail-Safe Timer shall be set to 1 minute

For Dry run / Low level protection:

Parameter	Comment
Fcn: Output Function	The Output Function shall be set to 5 (low alarm)
FLS: Fail-Safe Mode	The Fail-Safe Mode shall be set to 2 (high)
FSt: Fail-Safe Timer	The Fail-Safe Timer shall be set to 1 minute

Installation

- The two relay outputs or transistor outputs shall be connected in series.
- Relay version: The “n/o” and “com” contacts shall be used.

Reference

Pointek ULS200 Instruction Manual (see *Chapter 1.3*)

Protection against configuration changes

After configuration, the ULS200 lid shall be closed to protect the device against unwanted and unauthorized changes or operation.

Checking the safety function after installation

After installation you must test that the ULS200 is switching correctly. Operate the ULS200 under these conditions:

- that the predefined threshold value is exceeded (overflow)
- that the level falls below the predefined threshold value (dry run)

The ULS200 must deactivate the output.

3.5 Behavior in case of faults

Fault

The procedure in case of faults is described in the device Instruction Manual.

Return products

Defective devices should be sent to the Return Products 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.

See also

Services & Support (<http://www.siemens.com/automation/services&support>)

Partner (<http://www.automation.siemens.com/partner>)

3.6 Maintenance/Testing

Interval

We recommend that the functioning of the level transmitter be checked at regular intervals of one year.

Functional test

To ensure the proper operation of the ULS200, we recommend that the basic functionality of the ULS200 is tested as described in the Instruction Manual.

Functional safety proof test

To reveal possible undetected faults of the safety function, the entire SIF shall be tested according to IEC 61508 or 61511.

Inspect the antenna of the device and verify that no build-up of material has occurred. Clean the antenna if necessary.

To reveal dangerous undetected faults the ULS200 operates under these conditions:

- that the predefined threshold value is exceeded (overflow)
- that the level falls below the predefined threshold value (dry run)

The ULS200 must deactivate the output.

3.7 Safety characteristics

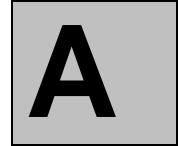
The safety characteristics necessary for use of the system are listed in the declaration of conformity (see Appendix). These values apply under the following conditions:

- The ULS200 is only used in safety-related systems with a low demand mode for the SIF.
- The safety-related parameters/settings (see *Settings* section) have been entered by local operation and checked before commencing safety-instrumented operation.
- The two relay-outputs or transistor-outputs shall be connected in series.
- Relay-version: The “n/o” and “com” contacts shall be used.
- The ULS200 is blocked against unwanted and unauthorized changes or operation.
- The average temperature viewed over a long period is ≤ 40 °C.
- All used materials are compatible with process conditions.
- Using the ULS200 correctly will maximize lifetime, because there are no known components which will prematurely wear. The maximum lifetime of the relay output is 150 000 switching cycles.
- The MTTR after a device fault is 8 hours.
- The minimum required time to react to a dangerous detected failure is 1 hour.

See also

Settings (*Chapter 3.4*)

SIL Declaration of Conformity (*Chapter A.1*)



A Appendix

A.1 SIL Declaration of Conformity



Industry

SIL Declaration of Conformity

Functional Safety according to IEC 61508 and IEC 61511

No. A5E02559297A - 03

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 ULS 200 Level Transmitter
Produktbezeichnung:	Type: 7ML1510-1**0*-Z C20 24 V DC, relay output
	7ML1510-2**0*-Z C20 24 V DC, transistor output
	7ML1510-3**0*-Z C20 100 to 230 V AC, relay output

We as manufacturer declare that the above identified devices are suitable for use in safety instrumented systems according to IEC 61508 / 61511. The device is capable of level measurements 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 proven in use assessment was carried out by exida GmbH according to IEC 61508 / IEC 61511. 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	Pointek ULS 200
Device Type	B
SIL Safety Integrity Level	1
HFT	0
PFDAVG	9.03*10 ⁻⁴
SFF Safe Failure Fraction	70 %
λ _{SD} Safe detected Failure Rate	0 FIT
λ _{SU} Safe undetected Failure Rate	361 FIT
λ _{DD} Dangerous detected Failure Rate	123 FIT
λ _{DU} Dangerous undetected Failure Rate	206 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 PFDAVG value is valid under the assumption of Mean Time To Restoration MTTR = 8h and Proof Test Interval T1 = 8760h.

Peterborough, July 02, 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 FMEDA and Proven-in-use Report (extract)

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the ultrasonic based process level switch Pointek ULS 200 with software version V9.10. Table 1 gives an overview of the different types that belong to the considered devices.

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.

★ Table 1: Types overview

Type	Description
7ML1510-1**0*	Standard version with DC power supply and relay output
7ML1510-2**0*	Standard version with DC power supply and transistor output
7ML1510-3**0*	Standard version with AC power supply and relay output
7ML1510-1C*0*	Ex version with DC power supply and relay output
7ML1510-2C*0*	Ex version with DC power supply and transistor output
7ML1510-3C*0*	Ex version with AC power supply and relay output

For safety applications only the described versions were considered. All other possible output variants or electronics are not covered by this report. The different devices can be equipped with or without display.

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

SIEMENS AG, A&D PI T2 and *exida* together did a quantitative analysis of the mechanical parts of the ultrasonic based process level switch Pointek ULS 200 to calculate the mechanical failure rates using *exida's* experienced-based data compilation for the different mechanical components of the ultrasonic based process level switch (see [D18] and [D19]). The results of this quantitative analysis were then added to the FMEDA results and sections 5.2 to 5.7 reflect the data for the complete level switch.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-2}$ to $< 10^{-1}$ for SIL 1 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 1 applications operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-01, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-02.

The ultrasonic based process level switch Pointek ULS 200 is considered to be a Type B¹ component with a hardware fault tolerance of 0.

For Type B components with a SFF of 60% to < 90% a hardware fault tolerance of 0 is sufficient according to table 3 of IEC 61508-2 for SIL 1 (sub-) systems.

¹ Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

* See Section 1.1 General for current Product Numbers and Descriptions.

As the ultrasonic based process level switch Pointek ULS 200 is supposed to be a proven-in-use device, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. The proven-in-use investigation was based on field return data collected and analyzed by SIEMENS AG, A&D PI T2. This data cannot cover the process connection. The proven-in-use justification for the process connection still needs to be done by the end-user.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6, the Type B the ultrasonic based process level switch Pointek ULS 200 with a hardware fault tolerance of 0 and a SFF of 60% to < 90% is considered to be suitable for use in SIL 1 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

The following tables show how the above stated requirements are fulfilled by the version with worse figures.

Table 2: IEC 61508 failure rates

λ_{SD}	λ_{SU}^2	λ_{DD}	λ_{DU}	SFF	DC _S ³	DC _D ³
0 FIT	361 FIT	123 FIT	206 FIT	70%	0%	37%

Table 3: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 9,03E-04	PFD _{AVG} = 4,50E-03	PFD _{AVG} = 8,98E-03

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 1 according to table 2 of IEC 61508-1 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-02.

The failure rates listed above do not include failures resulting from incorrect use of the ultrasonic based process level switch Pointek ULS 200, 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.

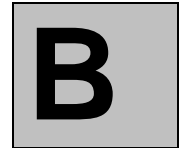
A user of the ultrasonic based process level switch Pointek ULS 200 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 5.2 to 5.7 along with all assumptions.

It is important to realize that the "no effect" failures are included in the "safe undetected" failure category according to IEC 61508, Edition 2000. 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 on the ultrasonic based process level switch Pointek ULS 200 (see Appendix 3).

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

³ DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.



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	
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.
SIF	Safety Instrumented Function	A portion of a safety instrumented system consisting of a sensor, logic solver/PLC and final element used to reduce the risk of occurrence of one hazardous event.
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.
TI	Proof Test Interval	Interval at which the test to reveal undetected faults is performed.
MooN	"M out of N" voting	Safety instrumented system, or part thereof, made up of "N" independent channels, which are so connected, that "M" channels are sufficient to perform the safety instrumented function. 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 non-functional status.

Example:

The measurement device reports a value 10% below the actual value, preventing the safety function from acting on a value, which is too high.

Low Demand Mode

The frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof-test frequency.

Safety function

Defined function of a device or system with the objective of achieving or maintaining a safe state of a system taking into account a defined dangerous occurrence.

Example:

Level / pressure / temperature measurement using 4-20mA output.

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 solver/ control system (PLC) and final element.

Definition: Safety Instrumented Function (SIF)

A portion of a safety instrumented system consisting of a sensor, logic solver/ control system (PLC) and final element used to reduce the risk of occurrence of one hazardous event.

Example:

A safety PLC will close a valve if the measured value exceeds a specified value.

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

© Siemens Milltronics Process Instruments Inc. 2009
Subject to change without prior notice



Printed in Canada

Rev. 2.0