Functional Safety Manual · December 2008

million
in one

sitrans
LR200

SIEMENS

SIEMENS

SITRANS

Level Instruments

Functional safety for SITRANS LR200

Product Information

SITRANS LR200:

7ML5422-010**	Uni-Constr polyprop. rod antenna version; 4 to 20mA HART
7ML5422-110**	
7ML5423-***-0A****	Flange Adapter/Rod Antenna Version; 4 to 20mA HART
7ML5423-***-1A****	
7ML5424-***-0A****	Flange Adapter, Sanitary Version; 4 to 20mA HART
7ML5424-***-1A****	
7ML5425-*0*-0*****	Flange Adapter/Horn Antenna Version; 4 to 20mA HART
7ML5425-*0*-1*****	

Ordering Number: 7ML5422####
12/2008

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.

Table of contents

1 Introduction

1.1 Safety Manual Revision History

Revision	Document Part Number	Release Date	Revision Comments
1.0	7ML19985KD01	12/07/2007	Initial Release
2.0	7ML19985KD02	19/12/2008	Clarification of product numbering for product versions covered by SIL Declaration of Conformity: Sections 1.1, Appendix A1 and A2.

1.2 General

The following table lists all available SITRANS LR200, 4 to 20 mA HART models:

Type of Antenna / Process Connection	Product Number
Uni-Constr polyprop. rod antenna version	7ML5422-0**10 7ML5422-1**10
Flange Adapter/Rod Antenna Version	7ML5423-*****-0A** 7ML5423-*****-1A**
Flange Adapter, Sanitary Version	7ML5424-*****-0A** 7ML5424-*****-1A**
Flange Adapter/Horn Antenna Version	7ML5425-***0*-0*** 7ML5425-***0*-1***

The term LR200 is used in the following text for all device models.

1.3 Purpose of this document

This document contains information and safety instructions required when using the LR200 in safety-instrumented systems.

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

1.4 Required documentation

This document deals with the “Continuous Radar Measurement – SITRANS LR200” exclusively as part of a safety function. This document only applies in conjunction with the following documentation:

No.	Name	Order No*
/1/	7ML5422 … 7ML5425: Instruction manual for HART/mA devices	7ML1998-5FN04 (English) 7ML1998-5FN11 (French) 7ML1998-5FN34 (German)

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

1.5 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	System integration	Installation path for PDM
01 04/2007	Firmware Rev. 2.03	From PDM V 5.2	Sitrans_LR200

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 (A5E0069####-0#) Safety manual order #: 7ML19985KD01
02 12/2008	 Safety manual order #: 7ML19985KD02

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 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 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 sensor, logic solvers or control systems (PLCs), and final elements.

Control system

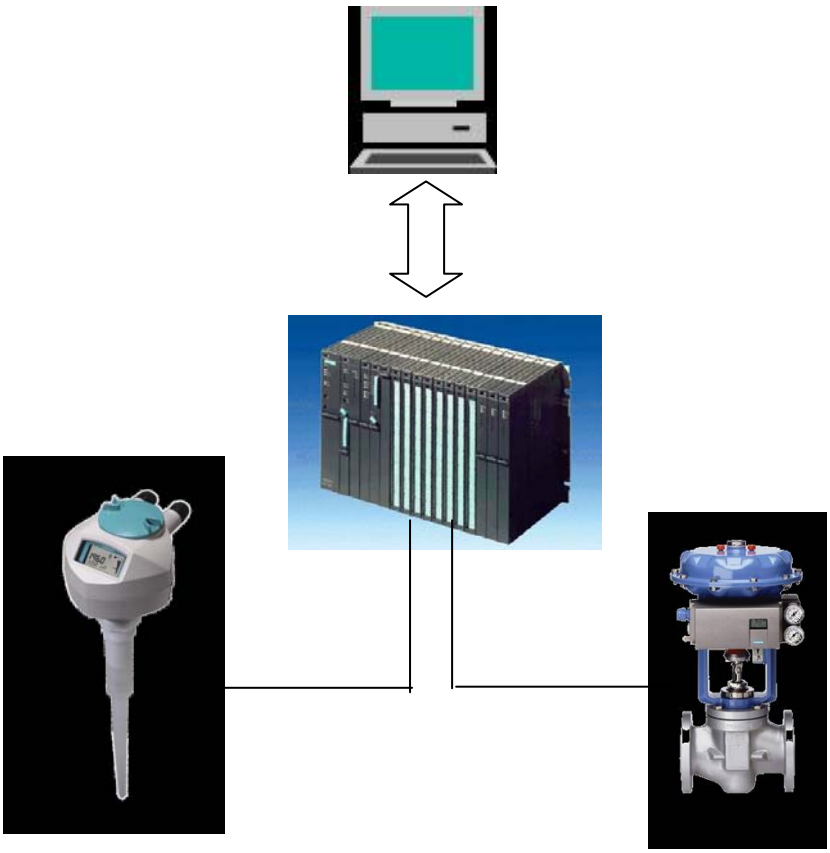


Figure 2-1: Example of a safety-instrumented system

Device operation

The LR200 is a 2-wire loop-powered, continuous level measuring instrument. The measured level is converted to a 4 to 20 mA signal. The safety PLC monitors the signal to perform a specified action based on the level measurement.

If the safety PLC detects a failure in the measurement device, it generates a failure signal, which brings the valve to the defined safe position.

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

Table 2-1 Safety Integrity Level

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

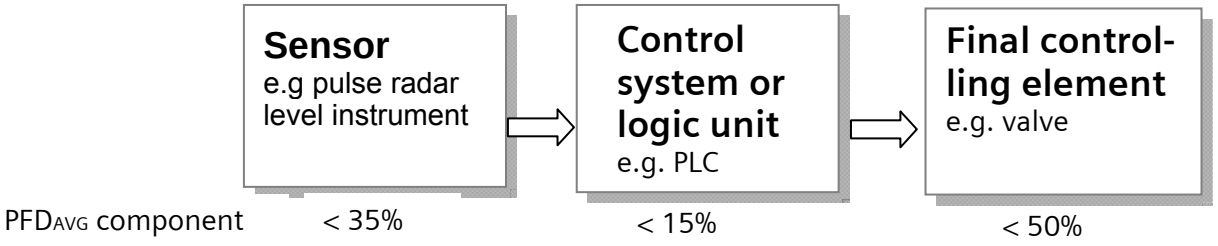


Figure 2-2 Example of PFD distribution

The table below shows the achievable Safety Integrity Level (SIL) for the entire safety-instrumented system for type B systems depending on the safe failure fraction (SFF) and the hardware fault tolerance (HFT). Type B systems include analog transmitters and shut-off valves 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

The achievable SIL is also constrained by the integrated set of techniques and measures used to ensure Systematic Safety Integrity, or avoidance of failures in design.

3 Device-specific safety instructions

3.1 Applications

The Hardware assessment of the SITRANS LR200 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 LR200 satisfies the hardware safety integrity requirements up to SIL1 in accordance with IEC 61508 and IEC 61511-1.

3.2 Safety function

The analog output 4to20 mA (NAMUR) may be used as part of a safety instrumented function (SIF). A dangerous failure is defined as a deviation of the output current from the actual measurement of ±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 LR200 in a SIF is 10[1] years. After this time, the device must be replaced.

Reference

LR200 Instruction manual (*Chapter 1.4*)

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 operating 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

Installation and configuration of the SITRANS LR200 (HART) must be completed following the instructions detailed in the device's Instruction Manual. All application limitations and restrictions described in that manual must be observed. False echo suppression must be enabled and properly configured.

Before being put into service, measurement by the SITRANS LR200 (HART) must be verified as accurate over the entire operating range, from empty to full. This will ensure that the device has been configured properly to avoid measurement error due to obstructions in the tank.

A high level trip point must have a distance from the blanking region of the device of greater than 2% of the measurement span. If the material reaches the blanking region an incorrect measurement may occur.

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 via LR200 menu:

Parameter	Set	Comment
P070	1	The Fail-Safe Timer shall be set to 1 minute
P071	4	User-selected value (defined in P073) for mA fail safe level
P073	note 1	The output current shall be set to 3.6 mA or 22.6 mA

NOTE 1: No changes are required; default is 22.6 mA.

Reference

SITRANS LR200 Instruction Manual (*Chapter 1.4*)

Protection against configuration changes

After configuration, the LR200 must be protected against unwanted and unauthorized changes/operation. The P000 parameter must be set to “Locked: programming not permitted.”

Checking the safety function after installation

After installation of the SITRANS LR200, a safety function proof test must be carried out (see *Chapter 3.6*).

When performing this test, measurement must be verified to be within a range of ±2% (full span) of the expected result.

3.5 Behavior in case of faults

Fault

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

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.

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 LR200, we recommend that the basic functions of the LR200 are 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.

To reveal dangerous undetected faults the LR200 analogue output shall be tested using the following procedure:

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Inspect the antenna of the device and verify that no build up of material has occurred. Clean the antenna if necessary according to the Instruction Manual.
3	Generate or simulate an alarm condition to force the LR200 to go to the high alarm current output and verify that the analog current reaches that value.
4	Generate or simulate an alarm condition to force the LR200 to go to the low alarm current output and verify that the analog current reaches that value.
5	Perform a two-point calibration of the LR200.
6	Perform a reference measuring with at least one measuring point between min and max level. The expected result must have a tolerance of not more than 2%.
7	Restore the loop to full operation.
8	Remove the bypass from the safety PLC or otherwise restore normal operation.

Table 3-1 Steps for Proof Test

The proof test interval (TI) is specified for the failure rate calculation of each individual SIF in a system (PFD_{AVG}). The TI must be at least once per year, or at least twice per expected demand interval. A TI of once per month is recommended.

3.7 Safety characteristics

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

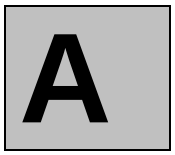
- The LR200 is only used in safety-related systems with a low demand mode for the SIF.
- The safety-related parameters/settings (see *Settings* section) have been entered by local operation and checked before commencing safety-instrumented operation.
- The LR200 is blocked against unwanted and unauthorized 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 logic solver (PLC) has to be configured to detect over range (> 21 mA) and under range (< 3.6 mA) failure of the LR200 (Fail High and Fail Low) and will recognize these as internal failure of the device.
- The LR200 assessment does not include an assessment of systematic safety integrity (software and development process).

See also

Settings (*Chapter 3.4*)

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

A Appendix



A.1 SIL Declaration of Conformity

SIEMENS

SIL Declaration of Conformity

Functional Safety according to IEC 61508 and IEC 61511

Siemens AG
Industry Automation
Sensors and Communication
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Siemens Milltronics
1954 Technology Drive
Peterborough, Ontario
K9J 7B1 / Canada

Product: **SITRANS LR200:**

7ML5422-0**10, 7ML5422-1**10	Uni-Construction polypropylene rod antenna version; 4..20mA HART
7ML5423-*****-0A**, 7ML5423-*****-1A**	Flange Adapter/Rod Antenna Version; 4..20mA HART
7ML5424-*****-0A**, 7ML5424-*****-1A**	Flange Adapter, Sanitary Version; 4..20mA HART
7ML5425-***0*-0***, 7ML5425-***0*-1***	Flange Adapter/Horn Antenna Version; 4..20mA HART

We as manufacturer declare that the LR200 Hardware is suitable for use in safety instrumented systems according to IEC 61508 / 61511. The device is capable of level measurement with an accuracy of 2% of full span for a safety instrumented function of Safety Integrity Level (SIL) 1. The provided Functional Safety Application Manual shall be observed.

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

Product revisions will be carried out by the manufacturer in accordance with IEC 61508.

Safety Related Characteristics SITRANS LR 200

SIL Safety Integrity Level	**1**
Device Type (IEC 61508)	**B**
HFT	**0**
λ_{SD} Safe detected Failure Rate	**0 FIT**
λ_{SU} Safe undetected Failure Rate	**540 FIT**
λ_{DD} Dangerous detected Failure Rate	**801 FIT**
λ_{DU} Dangerous undetected Failure Rate	**349 FIT**
PFD_{AVG}	$1.53*10^{-3}$
SFF Safe Failure Fraction	**70 %**

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

Peterborough, 2008, December 18th

Siemens AG

S. Woodward

Steven Woodward, VP of Technology

Martin Michler, I IA SC Functional Safety Manager

No. A5E02436696A-01

A.2 *FMEDA* Report (extract)

Management summary

This report summarizes the results of the hardware assessment carried out on the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output and software version V2.03. Table 1 gives an overview of the different versions 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: Version overview**

Type	Description
7ML5422-***10	SITRANS LR 200, Uni-Contruction polypropylene rod antenna version; 4..20mA HART
7ML5423-*****-*A**	SITRANS LR 200, Flange Adapter/Rod Antenna Version; 4..20mA HART
7ML5424-*****-*A**	SITRANS LR 200, Flange Adapter, Sanitary Version; 4..20mA HART
7ML5425-**0*-****	SITRANS LR 200, Flange Adapter/Horn Antenna Version; 4..20mA HART

For safety applications only the 4..20 mA output was considered. All other possible output variants or electronics are not covered by this report.

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

SIEMENS did a quantitative analysis of the mechanical parts of the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output to calculate the mechanical failure rates using *exida*'s experienced-based data compilation for the different mechanical components (see [D14]). 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 $\geq 10^{-2}$ 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 application the total PFD_{AVG} value of the SIF should be smaller than 1,00E-01, hence the maximum allowable PFD_{AVG} value for the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output would then be 3,50E-02.

The radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output is considered to be a Type B[1] component with a hardware fault tolerance of 0. For Type B components with a hardware fault tolerance of 0, the SFF has to be between 60% and 90% according to table 3 of IEC 61508-2 for SIL 1 (sub-) systems.

It is assumed that the connected logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output communicates detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures.

[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 1.2 General for current Product Numbers and Descriptions

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 40ºC. 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.

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 following tables show how the above stated requirements are fulfilled for the worst case configuration.

Table 2: Summary Ex version – Failure rates [2]

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**801**
Fail detected (internal diagnostics or indirectly [3])	496
Fail High (detected by the logic solver)	244
Fail low (detected by the logic solver)	61
Annunciation Detected	0
Fail Dangerous Undetected	**349**
Fail undetected	343
Annunciation Undetected	6
No Effect	**540**
Not part	**477**

Table 3: Summary Ex version – IEC 61508 failure rates

λ_{SD}	λ_{SU} [4]	λ_{DD}	λ_{DU}	SFF	DC_S [5]	DC_D [5]
0 FIT	540 FIT	801 FIT	349 FIT	79%	0%	69%

Table 4: Summary Ex version – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,53E-03	PFD_{AVG} = 7,61E-03	PFD_{AVG} = 1,51E-02

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.

[2] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

[3] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

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

[5] DC: Diagnostic coverage (safe or dangerous) for the radar transmitter by the safety logic solver.

As the Safe Failure Fraction (SFF) is above 60%, also the architectural constraints requirements for SIL 1 of table 3 of IEC 61508-2 for Type B subsystems with a Hardware Fault Tolerance (HFT) of 0 are fulfilled.

The failure rates listed above do not include failures resulting from incorrect use of the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output.

A user of the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output 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.

The failure rates are valid for the useful life of the radar transmitter SITRANS LR 200 (HART) with 4..20 mA current output (see Appendix 2).

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 on 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 to 20 mA 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 (PFDAVG)
- 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

7ML19985KD02
Printed in Canada

Rev. 2.0