

SIEMENS

SITRANS

Temperature transmitter Functional safety for SITRANS TW

Product Information

Introduction

1

General safety instructions

2

Device-specific safety
instructions

3

Appendix

A

List of
Abbreviations/Acronyms

B

Supplement to Operating Instructions 7NG3242

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

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

Table of contents

1	Introduction.....	5
1.1	Purpose of this document	5
1.2	Scope of this document	5
1.3	History	5
1.4	Further information.....	6
2	General safety instructions	7
2.1	Safety-instrumented system	7
2.2	Safety Integrity Level (SIL).....	8
3	Device-specific safety instructions	11
3.1	Application range	11
3.2	Safety function	12
3.3	Settings	13
3.4	Behavior in case of faults.....	14
3.5	Maintenance/Checking	14
3.6	Safety characteristics	15
A	Appendix.....	17
A.1	Literature and standards	17
A.2	SIL Declaration of Conformity	18
A.3	Test report (excerpt)	19
B	List of Abbreviations/Acronyms.....	23
B.1	Abbreviations	23
	Glossary	25
	Index.....	27

Tables

Table 2-1	Safety Integrity Level	8
-----------	------------------------------	---

Introduction

1.1 Purpose of this document

This document contains information and safety notes that you will require when using the device in safety-instrumented systems.

It is aimed at persons who install the device mechanically, connect it electrically, parameterize and commission it, as well as at service and maintenance engineers.

1.2 Scope of this document

documentation

This document deals with the temperature transmitter exclusively as a part of a safety function.

This documentation is applicable only in connection with the following documentation:

No.	Name	Order no.
/1/	Operating Instructions for SITRANS TW 7NG3242	A5E00054075

1.3 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 11/2006	FW: from 16.01.04	From PDM V 5.9	SITRANS TW

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

Edition	Remark
01 11/2006	First edition

1.4 Further information

Information

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

The content reflects the technical status at the time of printing. We reserve the right 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 Programming Manual is an integral part of the companion CD, which may be ordered separately. In addition, the Programming Manual is available on the Internet on the Siemens homepage.

On the CD you will also find the technical data sheet containing the ordering data, the Device Install software for SIMATIC PDM for subsequent installation and the required software.

See also

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

Instructions and Manuals (<http://www.siemens.com/processinstrumentation/documentation>)

Product information on SITRANS T in the Internet (<http://www.siemens.com/sitranst>)

General safety instructions

2.1 Safety-instrumented system

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

Description

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

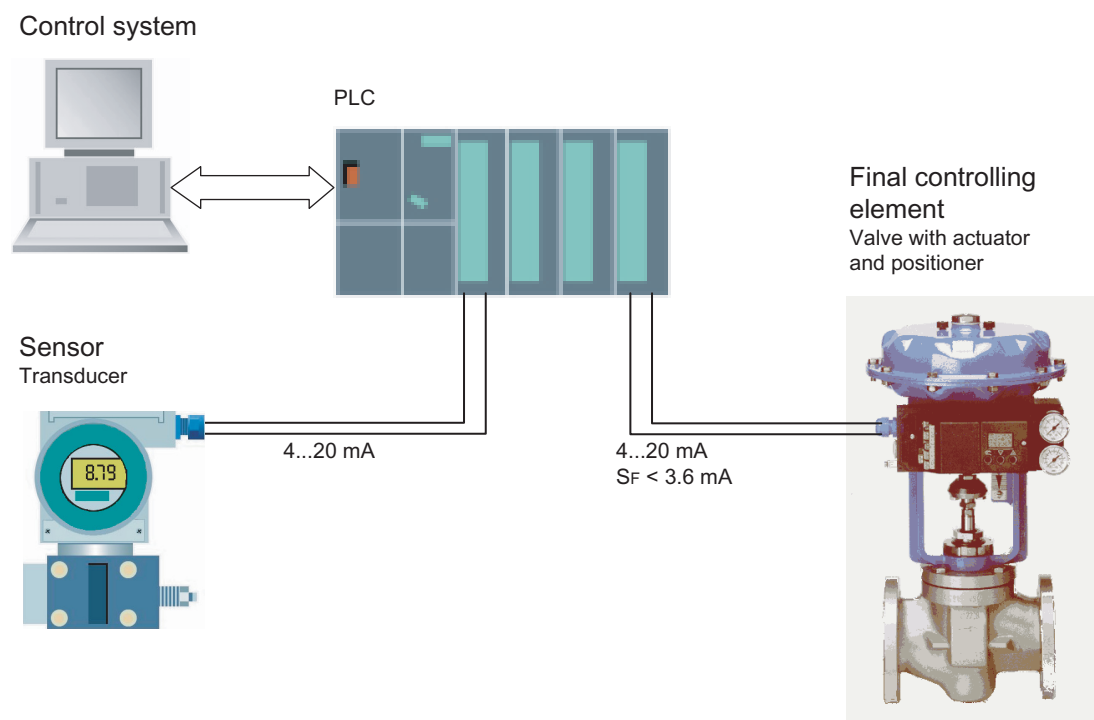


Figure 2-1 Example of a safety-instrumented system

S_F Failure signal

Functioning of the system as shown in the example

The transmitter generates a process-specific analog signal. The downstream control system monitors this signal to ensure that it does not fall below or exceed a set limit value. In case of a fault, the control system generates a failure signal of $< 3.6 \text{ mA}$ or $> 22 \text{ mA}$ for the connected positioner, which switches the associated valve to the specified safety position.

2.2 Safety Integrity Level (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.

Description

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

Table 2-1 Safety Integrity Level

SIL	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 system" (PFD_{AVG}) is normally split between the three sub-systems in the following figure.

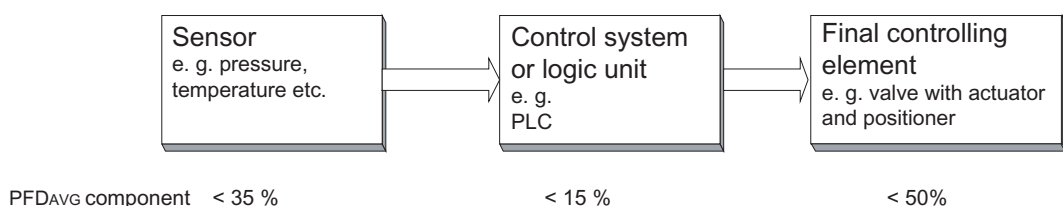


Figure 2-2 Example of PFD distribution

The following table shows the achievable Safety Integrity Level (SIL) for the entire safety-instrumented system for type B subsystems depending on the safe failure fraction (SFF) and the hardware fault tolerance (HFT). Type B subsystems include analog transmitters and shut-off valves without complex components, e.g. microprocessors (also see IEC 61508, Section 2).

SFF	HFT		
	0	1 (0) ¹⁾	2 (1) ¹⁾
< 60 %	Not permitted	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, limiting values, etc.
- The configuration level of the firmware is blocked against unauthorized operation.
- The function requires SIL of less than 4.

The transmitter fulfills these conditions.

Device-specific safety instructions

3.1 Application range

Overview

The SITRANS TW 4-wire bearing rail device is a transmitter with a universal input circuit. You can connect the following sensors and signal sources:

- Resistance thermometer
- Thermocouples
- Resistance-type transmitter/potentiometer
- mV sender
- As a special variant:
 - V sender
 - Power sources



Warning

The SITRANS TW 4-wire bearing rail device transmitter is a maintained device. It can be installed as an appropriate operation resource always only outside the hazardous area.

The transmitters in the "protection type - intrinsically safe" version have an EC type examination certificate and comply with the appropriate harmonized European CENELEC standards. They can be used to measure process variables in areas at risk for gas explosions (Zone 1, 0). A measurement of process variables in Zone 0 is permitted only if the sensors for Zone 0 are permitted as well.

The transmitter may also be used in areas at risk for dust explosions of Zones 20 and 21. In these cases it must be made certain that the devices attached to this electric circuit meet the requirements for the category 1D or 2D and are accordingly certified.

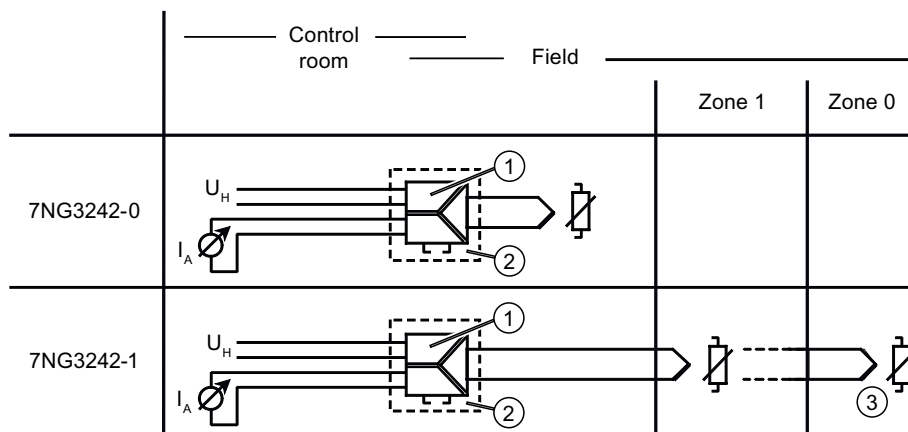


Figure 3-1 Areas of application of the transmitters in ex- and non-ex-versions

- ① Transmitter
- ② Field housing (if necessary, commercially available)
- ③ Only in connection with the specified protection requirements for the sensor

Requirements

The temperature transmitter meets the following requirements:

- Functional safety to SIL 1 under IEC 61508 or IEC 61511-1, from firmware version FW: from 16.01.04
- Explosion protection for corresponding versions
- Electromagnetic compatibility in compliance with EN 61326

3.2 Safety function

Safety function for the temperature transmitter

Measuring temperature is the safety function with the temperature transmitters. It is applicable for output current from 4 to 20 mA and ensures an accuracy of $\pm 2\%$ of the measured value in this range.



Warning

The binding settings and conditions are listed in the following chapters:

Settings (Page 13)

Safety characteristics (Page 15)

These conditions must be met in order to fulfil the safety function.

See also

Safety characteristics (Page 15)

3.3 Settings

The following settings are valid for the following SITRANS TWs:

- with current output "4..20 mA"
- Temperature measurement with a resistance thermometer or thermocouple

If your device does not meet the requirements specified above, you can also find in the description how to convert the device.

The following settings must be adhered to after installing and commissioning as per the Operating Instructions:

Operation/configuration

While operating/configuring, ensure that the technical data of the temperature transmitter are adhered to in their respective version.

Convert device to current output

1. If your device is set to voltage output, then open the device.
2. Open the jumper plugs X6 and X7 and close the jumper plug X8.

Check parameters

If your device is set to voltage output, then convert the device to current output. In SIMATIC PDM under "Output parameters - analog output", you set the parameter "Aoutput type" to "mA".

If your device is set to current output "0..20mA", then in SIMATIC PDM, set the parameter "Aoutput mode" under "Output parameters - analog output" to "4..20mA".

Checking the safety function

We recommend that:

- You check the status for warnings and alarms.
- Check the upper and lower alarm current value.
- Perform a 2-point calibration.
- You check the measuring accuracy that must be in the range of $\pm 2\%$ for the safety function. You check the measuring accuracy, for example, with a sensor calibration.

Protection against configuration changes

After parameterizing/commissioning:

Close the shorting plug X9.

Operation via HART communication is thus blocked.

Reference

You can find the operating instructions in the following documentation:

Operating Instructions for SITRANS TW 7NG3242

Order number A5E00054075

3.4 Behavior in case of faults

Repairs

Defective devices should be sent in 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 rating plate.

The address of the responsible SIEMENS repair center, contacts, spare parts lists, etc. can be found on the Internet.

See also

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

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

3.5 Maintenance/Checking

Interval

We recommend that the functioning of the temperature transmitter is checked at regular intervals of one year.

Checking the safety function

We recommend that:

- You check the status for warnings and alarms.
- Check the upper and lower alarm current value.
- Perform a 2-point calibration.
- You check the measuring accuracy that must be in the range of $\pm 2\%$ for the safety function. You check the measuring accuracy, for example, with a sensor calibration.

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 the calculation for each individual safety circuit in a system (PFD_{AVG}).

3.6 Safety characteristics

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

- The SITRANS P pressure temperature transmitter is only used in applications with a low demand rate for the safety function (low demand mode).
- The communication with the HART protocol is used only for the following:
 - Device configuration
 - Reading diagnostic values
- The safety-relevant parameters/settings were entered before the safety-instrumented operation via HART communication.
Settings (Page 13)
- The safety function test is concluded successfully.
- The transmitter is blocked against unwanted and unauthorized changes/operation.
- The following conditions apply to the transmitter:
 - The output sends an current signal.
 - The current signal is in the range of 4 to 20 mA.
 - The current signal is evaluated by a safe system.
- The specified error rates apply for the typical demand of an industrial environment as in IEC 60654-1 class C. The IEC 60654-1 class C means a protected place of application, with an average temperature of 40°C for an extended period of time.
- The calculation of fault rates is based on a MTTR of 8 hours.

The calculated Mean Time Between Failures (MTBF) for the SITRANS T temperature transmitter is approximately 165 years.

The maximum application time of the SITRANS TW in a safety application is 57 years. Replace the device after this time.

See also

SIL Declaration of Conformity (Page 18)

Appendix

A.1 Literature and standards

No.	Standard	Description
/1/	IEC 61508 Section 1-7	Functional safety of following systems: <ul style="list-style-type: none"> • Safety-instrumented • Electrical • Electronic • Programmable Target group: Manufacturers and suppliers of equipment
/2/	IEC 61511 Section 1-3	Functional safety - Safety systems for the process industry Target group: Planners, constructors and users

A.2 SIL Declaration of Conformity

SIEMENS**Declaration of Conformity****Functional Safety according to IEC 61508 and IEC 61511**

Siemens AG
Automation & Drives
Sensors & Communication
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Product: **SITRANS TW universal transmitter:**
Ordering Nr. : 7NG3242-*A*** 115/230 V AC/DC
7NG3242-*B*** 24 V AC/DC

We as manufacturer declare that the following failure rates for the above identified devices may be used in the relevant calculations required for IEC 61508 / 61511 safety instrumented system (SIS) compliance. The device is capable of temperature 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. Product revisions will be carried out by the manufacturer in accordance with IEC 61508.

The proven in use was carried out by exida GmbH in accordance with IEC 61508 / IEC 61511.

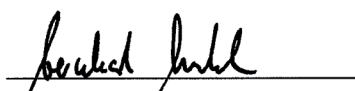
Safety Related Characteristics

Device Type	B
SIL Safety Integrity Level	1
HFT	0
PFD_{AVG}	8,57*10⁻⁴
λ_{SD} Safe detected Failure Rate	0 FIT
λ_{SU} Safe undetected Failure Rate	117 FIT
λ_{DD} Dangerous detected Failure Rate	204 FIT
λ_{DU} Dangerous undetected Failure Rate	196 FIT
SFF Safe Failure Fraction	62 %

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.

Karlsruhe, 2006, October 20th

Siemens AG



Bernhard Brendel, Manager R&D Temperature



Martin Michler, A&D SC Functional Safety Manager

No. A5E00982418A-01

A.3 Test report (excerpt)



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 temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output and software version V4.0.

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.

For safety applications only the 4..20 mA output was considered. Any 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.

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 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 temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output are considered to be Type B¹ components 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.

As the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output are supposed to be proven-in-use devices, 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 temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output with a hardware fault tolerance of 0 and a SFF of 60% to $< 90\%$ are 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.

It is assumed that the connected logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output communicate detected faults by an alarm output current $\leq 3,6mA$ or $\geq 21mA$. Assuming that the application program in the safety logic solver detects but does not automatically trip on these failures, these failures have been classified as dangerous detected failures.

The failure rates listed above do not include failures resulting from incorrect use of the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

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



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.

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

Table 1: Failure rates ²

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	204
Fail dangerous detected (internal diagnostics or indirectly ³)	87
Fail high (detected by the logic solver)	1
Fail low (detected by the logic solver)	115
Annunciation detected	1
Fail Dangerous Undetected	196
Fail dangerous undetected	193
Annunciation undetected	3
No Effect	117
Not part	160

Table 2: IEC 61508 failure rates

λ_{SD}	λ_{SU} ⁴	λ_{DD}	λ_{DU}	SFF	DC _S ⁵	DC _D ⁵
0 FIT	117 FIT	204 FIT	196 FIT	62%	0%	51%

Table 3: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 8,57E-04	PFD_{AVG} = 4,28E-03	PFD_{AVG} = 8,53E-03

A complete temperature sensor assembly consisting of the temperature transmitters SITRANS TW Series 7NG3242 and a thermocouple or RTD can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

Appendix 4 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

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



Assuming that the temperature transmitter SITRANS TW Series 7NG3242 will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution or the PFD_{AVG} value for the thermocouple or RTD in a low stress environment is as follows:

Table 4: SITRANS TW Series 7NG3242 / thermocouple (close coupled) in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
$PFD_{AVG} = 8,80E-04$	$PFD_{AVG} = 4,40E-03$	$PFD_{AVG} = 8,80E-03$	67%

$\lambda_{SD} = 0$ FIT

$\lambda_{SU} = 117$ FIT

$\lambda_{DD} = 299$ FIT

$\lambda_{DU} = 201$ FIT

Table 5: SITRANS TW Series 7NG3242 / 4-wire RTD (close coupled) in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
$PFD_{AVG} = 8,69E-04$	$PFD_{AVG} = 4,35E-03$	$PFD_{AVG} = 8,69E-03$	64%

$\lambda_{SD} = 0$ FIT

$\lambda_{SU} = 117$ FIT

$\lambda_{DD} = 251,5$ FIT

$\lambda_{DU} = 198,5$ FIT

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 $3,50E-02$.

A user of the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA 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 section 5.1 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 their 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 temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output (see Appendix 2).

List of Abbreviations/Acronyms

B.1 Abbreviations

Abbreviation	Full term in English	Meaning
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 Repair	Average period between the occurrence of a fault in 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
SFF	Safe Failure Fraction	Proportion of safe failures: Proportion of failures without the potential to bring the safety-instrumented system into a dangerous or non-permissible functional status.
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.
SIS	Safety Instrumented System	A safety-instrumented system (SIS) 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.
FIT	Failure in Time	Frequency of failure Number of faults withing 10 ⁹ hours
TI	Test Interval	Testing interval of the protective function

Abbreviation	Full term in English	Meaning
MooN	"M out of N" voting	<p>Classification and description of the safety-instrumented system in terms of redundancy and the selection procedures used.</p> <p>A safety-instrumented system or part that consists of "N" independent channels. The channels are connected to each other in such a way that "M" channels are in each case sufficient for the device to perform the safety instrumented function.</p> <p>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.</p>

Glossary

Dangerous failure

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

Fail-safe

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

Fault/failure

Failure:

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

Fault:

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

Fault

→ *Failure/fault*

Fault tolerance

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

Final controlling element

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

Risk

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

Safety function

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

Example:

Limit pressure monitoring

Safety Instrumented Function

→ *SIF*

Safety Integrity Level

→ *SIL*

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 limit signal sensor and a control valve.

Sensor

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

SIF

A part/function of a safety-instrumented system that reduces the risk of a dangerous failure occurring.

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 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 fractions (SFF)

Index

A

application time
 maximum, 15

C

characteristics
 Safety, 15
Checking, 14
Control system, 7

D

documentation
 Required, 5

F

Failure signal, 7
Final controlling element, 7
Firmware, 5

H

History, 5

M

Maintenance, 14
Mean Time Between Failures, 15

Measuring accuracy, 13
More information, 6
MTBF, 15
MTTR, 15

P

Product information on the Internet, 6

S

Safety
 Checking, 15
Safety function, 12
 Checking, 13, 14
Sensor, 7
Sensor calibration, 13
Settings, 13
Siemens Regional Office, 6

T

Technical data, 13

W

Write protection, 14

