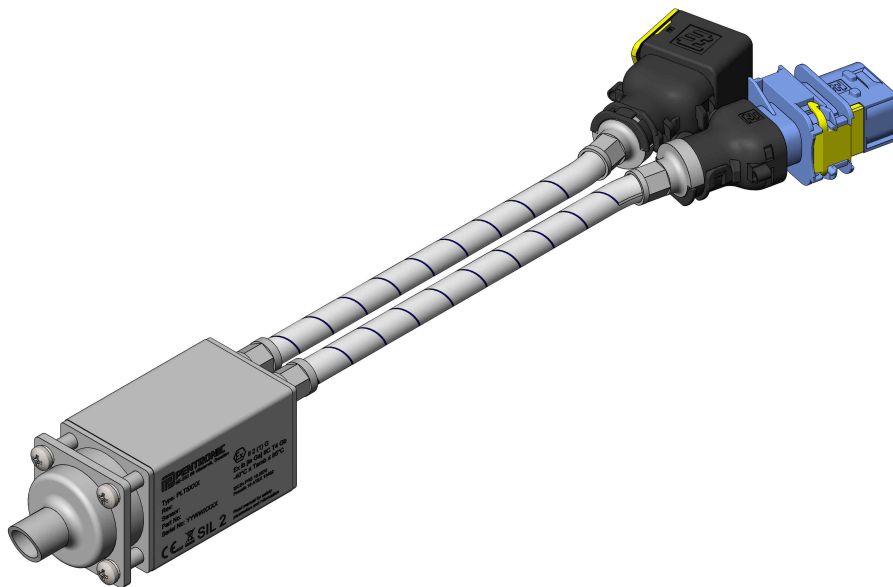


SIL Safety Manual

PLB5000 Temperature Transmitter

PLT5167, PLT5396, PLT5397



NOTICE: The information contained in this document is subject to change without notice.

In no event shall Pentronic AB be liable for errors contained herein or for indirect, incidental, special, consequential, reliance or cover damages, including loss of profits, revenue or data, incurred by any user or third party.

PLB is a registered trademark of Pentronic AB

Pentronic AB
Bergsliden 1
SE-593 96 Västervik
Sweden

Tel: +46 490 258500
info@pentronic.se
www.pentronic.se

Contents

1	General information	1
1.1	Technical and commercial support	1
1.2	About Pentronic AB	1
1.3	Document history	1
2	Introduction	2
2.1	Scope and purpose	2
2.2	Abbreviations and acronyms	2
2.3	Intended user	3
2.4	Documentation, standards and directives	4
3	Product description	5
3.1	Product marking	6
4	Installation	7
4.1	Constraints and limitations for use	7
5	Configuration	8
6	Functional test	8
7	Maintenance	8
8	Notification of failures	8
9	Decommissioning	8
10	Management of functional safety	9
10.1	Organization and resources	9
10.2	Safety planning	9
10.3	Implementation and monitoring	9
10.4	Configuration management	9
10.5	Design verification	9
11	Achievable SIL	10
11.1	Random hardware failures classification	10
11.1.1	Probability of failure	11
11.1.2	Diagnostic coverage (DC)	12
11.2	Architectural constraints	12
11.2.1	Safe failure fraction (SFF)	12
11.2.2	Hardware fault tolerance (HFT)	12
11.3	Control of systematic failures	13
12	Proof test	14
12.1	Proof test procedure	14

13 Device specific safety information	15
13.1 SIL certification	15
13.2 Safety function	15
13.3 Fault detection and reaction time (FDTR)	15
13.4 Safe state	15
13.5 Demand response time	15
13.6 Type classification	16
13.7 Mode of operation	16
13.8 Reliability data	17
13.8.1 Failure modes and failure rates for temperature sensor	18
13.9 Error Codes	18

List of Figures

3.1 Product marking of the PLT5167, PLT5396 and PLT5397 temperature transmitters 6

11.1 Example of PFD_{avg} /PFH distribution in subsystems 11

List of Tables

1.1 Document history	1
2.1 Abbreviations and acronyms	2
2.2 Product documentation	4
2.3 Associated directives	4
2.4 Associated standards	4
11.1 Correlation between SIL capability and PFD_{avg} and PFH	11
11.2 Safety Integrity Level relating to SFF and HFT for a type B element	12
13.1 Reliability data for one measurement channel, failure rates for sensor element not included	17
13.2 Failure modes for temperature sensors	18
13.3 Typical failure rates for temperature sensors	18
13.4 Transmitter error codes	19

1 | General information

1.1 Technical and commercial support

Pentronic AB

Bergsliden 1
SE-593 96 Västervik
Tel: +46 490-25 85 00
info@pentronic.se
www.pentronic.se

1.2 About Pentronic AB

Pentronic is one of Europe's largest manufacturers of industrial temperature sensors. In Scandinavia Pentronic is the leading supplier of equipment for temperature measurement to industry, research and education. Pentronic manufactures temperature sensors in its own facility, primarily Pt100 and thermocouples.

Pentronic collaborates with world leading manufacturers of calibration equipment, measurement and control instrumentation, optical temperature measurement and measurement equipment for moisture, thickness and flow.

1.3 Document history

See table 1.1 for correlation between product revision of the PLT5167, PLT5396 and PLT5397 temperature transmitters and the revision of this document. To locate the product revision of the transmitter see section 3.1.

Table 1.1: Document history

Document revision	Release date	Revision notes	Product type	Product revision
1.0 (56548)	2019-10-25	First release	PLT5167	1.0.X
			PLT5396	1.0.X
			PLT5397	1.0.X
1.1 (76238)	2025-06-19	Minor update	PLT5167	1.0.X
			PLT5396	1.0.X
			PLT5397	1.0.X

2 | Introduction

2.1 Scope and purpose

This Safety Manual provide guidelines, requirements and safety considerations related to the safety lifecycle phases of the Pentronic PLT5167, PLT5396 and PLT5397 temperature transmitters. The recommendations and requirements in this manual shall be considered and implemented during, installation, commissioning, operation and decommissioning of the transmitter.

The manual also provides guidance to quality systems, documentation and competence, but these requirements do not replace any of the end user company's quality systems, procedures and practices. Local statutory regulations, should they be stricter, shall always take precedence over this manual.

Annex D *Safety manual for compliant items* of IEC 61508-2 states that the purpose of the safety manual is to document all information needed to enable the integration of the product into a safety-related system, subsystem or element in compliance with the IEC 61508 standard.

2.2 Abbreviations and acronyms

Table 2.1: Abbreviations and acronyms

Acronym/Abbreviation	Designation	Description
DC	Diagnostic Coverage	Fraction of dangerous failures detected by on-line diagnostic tests
DRT	Demand Response Time	Maximum time from a temperature change in the sensor until the value is available for the PLT5000 temperature gateway.
EUC	Equipment Under Control	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities
FDTR	Fault Detection and Reaction Time	Maximum time for fault detection and until a safe state is set
FIT	Failures in Time	$FIT = 1 \times 10^{-9}$ failures per hour
FMEDA	Failure Modes, Effects and Diagnostic Analysis	A systematic analysis technique to obtain subsystem / product level failure rates, failure modes and diagnostic capability
Element		Part of a subsystem comprising a single component or any group of components that performs one or more element safety functions
HFT	Hardware Fault Tolerance	The ability of a functional unit to perform its intended function in case of faults and anomalies
MT	Mission Time	Is the time from plant start-up to the replacement of the product

Table 2.1 continues

Acronym	Designation	Description
MTBF	Mean Time Between Failure	Average time between two failures
MTTR	Mean Time To Restoration	Average time between the occurrence of a fault in the product until restoration of functionality
PFD_{avg}	Average Probability of Failure on Demand	The probability that a safety related function will fail to respond/react when a demand occurs
PFH	Probability dangerous Failure per Hour	The average frequency of dangerous failure per hour
PST	Process Safety Time	Period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the EUC or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring
PTC	Proof Test Coverage factor	A percentage of the effectiveness of the proof test, to detect dangerous undetected failures
SFF	Safe Failure Fraction	The fraction of the overall failure rate of a device that results in either a safe failure or dangerous detected failure
SIF	Safety Instrumented Function	A safety function with a specified SIL which is necessary to achieve functional safety
SIL	Safety Integrity Level	Safety Integrity level is a measure of performance required from a safety instrumented system to maintain or achieve the safety state. IEC 61508 defines four discrete levels SIL1...SIL4. Each level corresponds to a range of probability for failure of a safety function.
λ_{SD}	Safe Detected failure rate	Failure that causes the device to enter a fail safe state
λ_{SU}	Safe Undetected failure rate	Failure that causes the device to enter a fail safe state
λ_{DD}	Dangerous Detected failure rate	Dangerous failures that are detected by the internal diagnostic
λ_{DU}	Dangerous Undetected failure rate	Dangerous failures that are not detected by the device
λ_{FD}	Detectable fault detection error failure rate	Detectable failures that does not affect safety but could impact the ability to detect a future fault
λ_{FU}	Undetectable fault detection error failure rate	Undetectable failures that does not affect safety but could impact the ability to detect a future fault

2.3 Intended user

This manual is intended for all people involved in the life-cycle activities of Pentronic PLT5167, PLT5396 and PLT5397 temperature transmitters. The safety life cycle comprise all activities from the equipment arrives from Pentronic until it is safely disposed after the Mission Time (MT). System design, installation and commissioning of this device shall be performed by qualified personnel.

2.4 Documentation, standards and directives

The safety manual shall be read in conjunction with the product documentation stated in table 2.2.

Table 2.2: Product documentation

Document
<i>PLT5167, PLT5396, PLT5397 Ex Safety instructions</i>
<i>PLT5167, PLT5396, PLT5397 Data sheet</i>
<i>PLG5465 User manual</i>
<i>PLG5465 SIL Safety manual</i>

The PLT5167, PLT5396 and PLT5397 temperature transmitters adhere to the directives and standards stated in table 2.3 and table 2.4.

Table 2.3: Associated directives

Directive	Title
2014/30/EU	DIRECTIVE 2014/30/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility
2014/34/EU	DIRECTIVE 2014/34/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres
2011/65/EU	RoHS DIRECTIVE 2011/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, as amended by Directive (EU) 2015/863

Table 2.4: Associated standards

Standard	Title
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements
EN 61326-1:2013	Electrical equipment for measurement, control and laboratory use – EMC requirements– Part 1: General requirements
EN 61326-3-1:2009	Electrical equipment for measurement, control and laboratory use - EMC requirements- Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications
EN 55011:2009	Industrial, scientific and medical equipment - Radio frequency disturbance characteristics - Limits and methods of measurement with amendment EN 55011:2009/A1:2010
IEC 60079-0:2017	Explosive atmospheres – Part 0: Equipment – General requirements
IEC 60079-11:2011	Explosive atmospheres - Part 11: Equipment protection by intrinsic safety "i"

3 | Product description

The PLT5167, PLT5396 and PLT5397 temperature transmitters are universal isolated digital temperature transmitters, with a rugged design to be used in harsh environment. The transmitters are qualified to be a part of SIL2 Safety Instrumented Function (SIF) operating in high, continuous or low demand mode.

The transmitter is available with 1,2 or 3 independent measurement channels, PLT5167, PLT5396 respectively PLT5397. The temperature sensor/sensors are permanently mounted on the transmitter during production and is/are not exchangeable, the following sensor types are supported:

- Thermocouples
 - Type K
 - Type N
 - Type R
 - Type S
- RTD
 - Pt100 3-wire
 - Pt100 4-wire
 - Pt1000 3-wire
 - Pt1000 4-wire

The sensor inputs are galvanically isolated and can be used with sensors connected to local earth, without loss of accuracy due to interference.

The transmitter is a member of the PLB5000 temperature transmitter family and is one of the building blocks of a PLB5000 measurement system. It shall be used together with a Pentronic PLG5465 gateway. Such a gateway supports communication with a large number of PLB5000 temperature transmitters via a secure and very robust safety protocol. The gateway collects temperature values from the transmitter/transmitters and propagates them via the PROFIsafe protocol which is superimposed on the standard PROFIBUS protocol to a PLC. For more information regarding designing a measurement system with Pentronics PLB5000 temperature transmitters consult the *PLG5465 User manual* and *PLG5465 SIL Safety manual*.

The transmitter has two separate power supply connections and two independent bus connections hence there is a possibility to connect the product to two PLG5465 Temperature gateways and achieve cable redundancy in the installation.

NOTE! Connection and measurement channel redundancy shall not be taken in to account in SIL calculations for a transmitter, it shall be considered as a Type B Element with HFT = 0 (see section 11.2.2 and 13.7)

3.1 Product marking

Information regarding identification, sensor type etc is found on the transmitter side, see figure 3.1.

NOTE! For more information regarding the EX marking and installation in EX zone consult the *PLT5167, PLT5396, PLT5397 Ex Safety instructions*.



Figure 3.1: Product marking of the PLT5167, PLT5396 and PLT5397 temperature transmitters

- ① Transmitter type, i.e PLT5167, PLT5396 or PLT5397
- ② Product revision of transmitter
NOTE! Verify that the revision of this safety manual correlates with the revision on the product (see table 1.1)
- ③ Connected sensor type e.g thermocouple type K (TC K), PT100 4-wire etc
- ④ Transmitter part number
- ⑤ Transmitter serial number
- ⑥ EX-marking

4 | Installation

The transmitter shall be grounded at the installation point and directly to the exterior steel sensor measurement probe. The transmitter shall be isolated from incoming bus cables and should not be bonded over the connectors. If the transmitter shall be used in potentially explosive areas please consult the *PLT5167, PLT5396, PLT5397 Ex Safety instructions*.

4.1 Constraints and limitations for use

The transmitter has a ingress protection of IP65 and the ambient temperature during operation for the transmitter shall be between -40 and +85 C°. It is the responsibility of the designer of the SIF to verify that the transmitter complies with the expected environmental limits and ensure that ambient temperature of the application is within this limits. For more information regarding technical specification of the transmitter consult the *PLT5167, PLT5396, PLT5397 User manual*.

5 | Configuration

The transmitter has no local or remote configuration interfaces, all parameters such as sensor type, error codes etc are preconfigured from factory.

6 | Functional test

It is the responsibility of the end user to perform a functional test of the complete transmitter sensor assembly, prior to commissioning.

Before performing a functional test, ensure that all necessary site acceptance test procedures required to achieve safety are followed.

1. Bypass the safety function and take appropriate action to avoid a false trip.
2. Verify that the sensor temperature for each transmitter channel has its expected value.

NOTE! For proof test procedure see chapter 12

7 | Maintenance

There are no maintenance procedures for the transmitter. The transmitter is completely maintenance free.

8 | Notification of failures

In case of malfunction of the transmitter, the product shall be put out of service and the process held in a safe state by means of other measures. Pentronic AB must be informed when a transmitter is required to be replaced due to failure.

Please contact Pentronic AB at quality@pentronic.se and ask for the *Product return instructions* or visit www.pentronic.se for return form.

9 | Decommissioning

Prior to decommissioning the transmitter, proper planning and procedures shall be established. An analysis shall be performed to determine the impact on functional safety from the proposed decommissioning activities.

10 | Management of functional safety

This chapter provides information about typical management activities that are necessary, to ensure that the functional safety objectives are met during all phases of the products life cycle. The management activities with respect to Functional Safety shall be identified, documented and planned as part of an overall Functional Safety Management Plan. The Policy and Strategy for achieving safety is the responsibility of the end user and shall be identified and defined together with the means for evaluating its achievement. Application specific standards may contain other requirements for Functional Safety Management activities. Such requirements are not reflected in this manual.

10.1 Organization and resources

Persons, departments, organizations and other units involved in safety related activities such as design, engineering, installation, configuration, test, commissioning, maintenance and operation shall have sufficient level of safety knowledge, technical knowledge, skills and relevant experience to carry out the activities for which they are accountable.

It is the responsibility of the end user to ensure that all organizational units involved during any phase of the Safety Life Cycle of the products, possess sufficient competency.

10.2 Safety planning

Safety planning shall take place to define required activities, along with the persons, departments, organizations or other units responsible to carry out these activities.

10.3 Implementation and monitoring

Procedures shall be implemented for monitoring the safety performance of the installed safety equipment during the operation phase. Performance shall be verified against the requirements given in the related Safety Requirement Specification.

10.4 Configuration management

Procedures for configuration management shall be established and used during the whole life cycle of the transmitter. Configuration Management comprise the running of an inventory list, record the version of all safety products and their configuration, as well as the version of all utility software/tools used (see section 3.1 for how to locate the transmitter product revision).

10.5 Design verification

The achieved SIL capability of an entire SIF design must be verified by the designer. The designer must take for example PFD_{avg} /PFH, automatic diagnostics, PTC, T_p , MTTR of all products in the SIF into consideration. Each subsystem must be checked to assure compliance with the minimum hardware fault tolerance (HFT) requirements, systematic capability requirements etc.

11 | Achievable SIL

Safety is, in most situations, best achieved by an inherently safe process design. When this is not practicable, the residual risk shall be identified and handled by one or more protective systems. The overall safety requirements of a process are identified by carrying out a hazard and risk assessment.

The identified safety requirements are allocated to safety functions and related protection systems. For each identified SIF the Safety Integrity Level (SIL) shall be identified.

Important characteristics of a system, which implements one or several safety functions, are the response time during normal operation; Demand Response Time (DRT), and the response time during internal faults; Fault Detection and Reaction Time (FDRT). These characteristics of the system relates to the Process Safety Time (PST) of the process being controlled. For definitions of terms and abbreviations like DRT, FDRT and PST, see table 2.1.

The maximum SIL that can be claimed for an element is dependent on several factors:

- Quantitative requirements for random hardware failure
- Architectural constraints
- Control of systematic failures

For transmitter specific safety data see chapter 13.

11.1 Random hardware failures classification

According to IEC 61508 a failure in an element that affect its safety function can be either:

- A dangerous failure that:
 - prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or
 - decreases the probability that the safety function operates correctly when required
- A safe failure that:
 - results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or
 - increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state

These failure modes can either be detectable by diagnostics or undetectable and can be divided into the following types:

1. Total failure rate for dangerous detected failures (λ_{DD})
2. Total failure rate for dangerous undetected failures (λ_{DU})
3. Total failure rate for safe detected failures (λ_{SD})
4. Total failure rate for safe undetected failures (λ_{SU})

Furthermore IEC 61508 requires that the failure rate of the diagnostics shall be stated for an element. This kind of failure does not directly affect safety, but could impact the ability to detect a future fault i.e a fault in a diagnostic circuit and will be referred to as λ_{FD} (detectable) and λ_{FU} (undetetectable).

11.1.1 Probability of failure

IEC 61508 describes three modes of operation for a safety function:

1. Low demand mode, where the SIF is only performed on demand, in order to transfer the Equipment Under Control (EUC) into a specified state, and where the frequency of demands is no greater than one per year
2. High demand mode, where the SIF is only performed on demand, in order to transfer the EUC into a specified state, and where the frequency of demands is greater than one per year
3. Continuous mode, where the SIF retains the EUC in a safe state as part of normal operation

For high/continuous demand mode applications the failure rate to consider is the Probability of dangerous Failure per Hour (PFH), for low demand mode applications the corresponding failure rate is the average Probability of Failure on Demand (PFD_{avg}).

For a SIF that consists of input, logical, and output sub systems, the distribution of the failure rates PFD_{avg}/PFH for the sub systems are often defined according to figure 11.1.

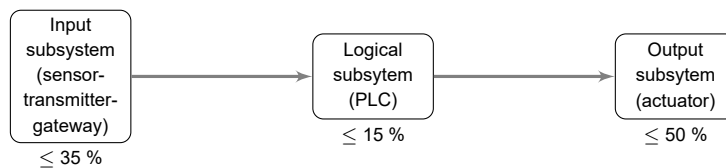


Figure 11.1: Example of PFD_{avg} /PFH distribution in subsystems

The achievable SIL for a SIF is dependent of the sum of PFH or PFD_{avg} for all sub systems in the SIF, see table 11.1.

Table 11.1: Correlation between SIL capability and PFD_{avg} and PFH

SIL	PFD_{avg}	PFH
4	$\leq 10^{-5}$ to $<10^{-4}$	$\leq 10^{-9}$ to $<10^{-8}$
3	$\leq 10^{-4}$ to $<10^{-3}$	$\leq 10^{-8}$ to $<10^{-7}$
2	$\leq 10^{-3}$ to $<10^{-2}$	$\leq 10^{-7}$ to $<10^{-6}$
1	$\leq 10^{-2}$ to $<10^{-1}$	$\leq 10^{-6}$ to $<10^{-5}$

An example how to calculate PFD_{avg} is described below.

$$PFD_{Avg} = \lambda_{DU} \times (PTC)\left(\frac{T_p}{2} + MTTR\right) + \lambda_{DU} \times (1 - PTC)\left(\frac{MT}{2} + MTTR\right) + (\lambda_{DU} \times MTTR)$$

11.1.2 Diagnostic coverage (DC)

The effectiveness of the on-line diagnostic of an element can be expressed as the ratio between the failure rate of detected dangerous failures and the total dangerous failure rate.

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$

11.2 Architectural constraints

According to IEC 61508 there are two possible routes to fulfill the standards requirements regarding architectural constraints.

- Route 1_H, where the achievable SIL is dependent of the safe failure fraction (SFF) and the hardware fault tolerance (HFT).
- Route 2_H, where the achievable SIL is dependent on component reliability data from feedback from end users, increased confidence levels and HFT for specified safety integrity levels.

IEC 61508 distinguishes between type A and type B elements, where a type A element is regarded as non-complex (all failure modes are well defined) and a type B element as complex (at least one failure mode is not well defined).

11.2.1 Safe failure fraction (SFF)

Safe Failure Fraction (SFF) is the ratio of safe (λ_S) and dangerous detected (λ_D) failures to the total failure rate. The higher SFF the lower the probability of failure. The key number in the SFF calculation is λ_{DU} , those errors that are not detected by online diagnostics and could result in a dangerous error in the element.

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

11.2.2 Hardware fault tolerance (HFT)

Hardware Fault Tolerance (HFT) is the ability of the element to continue to perform a required function in the presence of errors. A hardware fault tolerance of N means that N+1 error may result in that the element can not perform its intended function.

Table 11.2 can be used to determine the achievable SIL as a function of the Hardware Fault Tolerance (HFT) and the Safe Failure Fraction (SFF) for a type B element.

Table 11.2: Safety Integrity Level relating to SFF and HFT for a type B element

SFF: Safe Failure Fraction	HFT: Hardware Fault Tolerance		
	0	1	2
<60 %	Not permitted	SIL 1	SIL 2
60 ... ≤ 90 %	SIL 1	SIL 2	SIL 3
90 ... ≤ 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

11.3 Control of systematic failures

Systematic failures are failures that can not be predicted as an opposite to random hardware failures. A systematic failure is often caused by a design error and can only be eliminated by a modification of the design, operational procedures etc according to IEC 61508.

To minimize the risk of systematic failures in an element, the standard stipulates measures and techniques to be used during product design. The standard also requires that an element is designed to tolerate or control systematic failures during operation such as foreseeable human errors or environmental stresses.

The term systematic capability (SC) is used as a measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified safety function, when the element is applied in accordance with the instructions specified in the safety manual for the element.

12 | Proof test

The IEC 61508 defines a proof test as a *periodic test performed to detect failures in a safety related systems so that the system can be restored to an "as new" condition or close as practical to this condition.*

The objective of proof test is to detect possible dangerous undetected failures (λ_{DU}) in the transmitter that may compromise the SIF to do its intended function. λ_{DU} are failures which will not be detected by the automatic diagnostic checks in the transmitter.

It is under the responsibility of the end user to define the type of proof test and the interval time period. The proof test must be carried out by qualified personnel.

The proof test interval, is to be determined by the reliability calculations for the SIF and must be performed more frequently than or as frequently as specified in the calculation in order to maintain the required Safety Integrity of the SIF.

Results of the proof tests shall be documented.

NOTE! If any failures are detected during the proof test, the transmitter must be taken out of service and the safety of the process must be ensured by other means. Failures detected that compromise functional safety shall be reported back to Pentronic AB (see chapter 8).

12.1 Proof test procedure

A recommended proof test procedure is described below. This test will detect 95% of possible λ_{DU} failures in the transmitter.

Before performing a proof test, ensure that all necessary site acceptance test procedures required to achieve safety are followed.

1. Bypass the safety function and take appropriate action to avoid a false trip.
2. Power off the gateway
3. Connect one power supply and one bus
4. Perform a multi-point calibration (at least 2-points) of one transmitter channel, within the applications temperature range, and verify the measurement values in the PLC or web interface of the Pentronic PLG5465 Temperature gateway (see *PLG5465 SIL Safety manual*).
5. Repeat step 2...4 for secondary power supply and bus.
6. Repeat steps 2...5 for each transmitter channel.

13 | Device specific safety information

13.1 SIL certification

RISE - Research Institutes of Sweden has performed an full assessment of Pentronics transmitter against all applicable requirements in IEC 61508:2010 and the transmitter fullfills:

- Systematic capability: SC2
- Architectural constraints: SIL2 (Route 1_H, Type B element, HFT=0 and SFF_≥90%)
- Mode of operation: Continuous, High or Low

13.2 Safety function

A temperature value from a connected sensor is converted to a digital measurement value in the transmitter. The temperature value is then stored and is ready for transmit via a safety protocol to a Pentronic PLG5465 Temperature gateway.

13.3 Fault detection and reaction time (FDTR)

If the internal diagnostics in the transmitter detects an error (λ_{DD}), the transmitter will enter safe state. The maximum fault detection and reaction time (FDTR) is less than 30 seconds. The transmitter will stay in safe state until the error is resolved, for more information regarding error codes see section 13.9 In case of an error in the internal diagnostics (λ_{FU}) or that the error is not detected by the internal diagnostics (λ_{DU}) the transmitter may deliver an incorrect temperature value.

NOTE! If the transmitter is restarted and the error condition still persists it may take up to: start up time (15s) + FDTR (<30s) before safe state is entered.

13.4 Safe state

The transmitter may enter two types of safe state in case an error has been detected by the internal diagnostics:

1. No response to a request from a PLG5000 temperature gateway
2. An error code is transmitted instead of a temperature value up on request.

For more information regarding how a PLG5000 temperature gateway handles transmitter safe states see *PLG5465 SIL Safety manual*.

13.5 Demand response time

The maximum demand response time is less than 2 seconds. This is the maximum time from a temperature change in the sensor until the new value is available for the PLT5000 temperature gateway.

13.6 Type classification

This device is classified as a Type B element according to IEC 61508, with a Hardware Fault Tolerance (HFT) of 0.

13.7 Mode of operation

The transmitter is suitable for use in a high, continuous and low demand mode SIF.

If the transmitter is used in a high or continuous mode the fault tolerance time of the complete system must be higher:

- Than the sum of the reaction times.
- Than the diagnostic test intervals of all components in the safety-related measurement chain.
- Than the the ratio of the diagnostic test rate to the demand rate equals or exceeds 100 .

According to IEC 61508-2:2010 7.4.4.1.4.

13.8 Reliability data

The failure rates of the electronics in the transmitter has been determined by a FMEDA, with component failure rates retrieved from the Siemens standard SN 29500.

Failure rate data listed in table 13.1 are only valid for the useful life time of the transmitter, reliability calculations based on the failure rates for the transmitter for mission times beyond the lifetime may result in that the calculated SIL level for the SIF will not be achieved.

The following assumptions has been made during the FMEDA analysis:

- The Mean Time to Repair (MTTR) after a device failure is 8 hours.
- Based on manufacturers component data, a useful life time is set to 15 years hence is the Mission Time (MT) set to 15 years in the FMEDA calculations. If plant experience indicates a shorter lifetime, that time should be used instead.
- Failure rates are constant, wear out mechanics are not included
- The PTC is 95%.
- Safe failures are regarded as dangerous failures with a diagnostic coverage of 99%
- The device is installed according to manufactures instruction.
- The transmitter is a Type B element with a HFT of 0.
- External power supply failures are not considered.
- Ambient temperature 40 °C.
- The failure rate for the sensor element is not included (see section 13.8.1 for typical reliability data for temperature sensors)

Table 13.1: Reliability data for one measurement channel, failure rates for sensor element not included

Transmitter input	Failure rates (FIT)						DC(%)	SFF(%)	PFH (% of SIL2 budget)	PFD _{avg} with T _p = (% of SIL2 budget)		
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{FD}	λ_{FU}				1 year	2 years	5 years
RTD 3-wire	0	0	830	34	2	13	96.1	96.1	3.4	2.6	4.0	8.2
RTD 4-wire	0	0	831	35	2	13	96.0	96.0	3.5	2.7	4.1	8.5
Thermocouple	0	0	836	34	3	13	96.1	96.1	3.4	2.6	4.0	8.3

NOTE! The failure rates for all elements in a SIF shall be considered, hence SFF, PFH, DC and PFD_{avg} values in table 13.1 shall be regarded as reference values only. It is the responsibility of the SIF designer to calculate SFF, PFH, DC and PFD_{avg} values for respectively SIF.

13.8.1 Failure modes and failure rates for temperature sensor

Temperature sensors are not covered by IEC 61508, the scope of IEC 61508 states:

1.2 In particular, this standard

a) applies to safety-related systems when one or more of such systems incorporates electrical/electronic/programmable electronic elements;

To be able to calculate values for SFF, PFD_{avg} etc. for the complete transmitter sensor assembly, failure rates and failure modes of the temperature sensor must be taken into account. The transmitter supports two types of temperature sensors; thermocouple and resistance thermometers (RTD). Failure modes and typical failure rates for temperature sensors are described in table 13.2 and 13.3.

Table 13.2: Failure modes for temperature sensors

Sensor type	Failure mode			
	Sensor drift	Short circuit	Open circuit	Wire resistance difference
RTD 3-wire	λ_{DU}	λ_{DD}	λ_{DD}	λ_{DU}
RTD 4-wire	λ_{DU}	λ_{DD}	λ_{DD}	N/A
Thermocouple	λ_{DU}	λ_{DU}	λ_{DD}	N/A

Typical failure rates for temperature sensors compatible with the transmitter are listed in table 13.3. If plant experience indicates different failure rates these rates shall be used instead. The failure rates depends on the following parameters:

Sensor type:

- RTD 3-wire
- RTD 4-wire
- Thermocouple

Mechanical stress:

- High vibration > 0.1g
- Low vibration < 0.1g

Sensor connection:

- Close couple (< 30 cm)
- Extension wire (≥ 30 cm)

Table 13.3: Typical failure rates for temperature sensors

Sensor environment	RTD 3-wire Failure rates (FIT)		RTD 4-wire Failure rates (FIT)		Thermocouple Failure rates (FIT)	
	λ_{DU}	λ_{DD}	λ_{DU}	λ_{DD}	λ_{DU}	λ_{DD}
Low Stress - Close coupled	9	39	3	48	5	95
Low Stress - Extension wire	95	380	5	495	100	900
High Stress - Close coupled	173	787	50	950	100	1900
High Stress - Extension wire	1900	7600	100	9900	2000	18000

13.9 Error Codes

If an error is detected in the transmitter, the transmitter will respond with an error code instead of a temperature value to a request from a PLG5465 gateway. The gateway will then forward the error code to the control system via PROFIsafe over PROFIBUS. For more information see *PLG5465 SIL Safety manual*.

Table 13.4: Transmitter error codes

BIT	Abbreviation	Error Description
0	ERR_INTERNAL	Internal error
1	ERR_SENSOR_TEMP_OVER_RANGE	Possible causes: • Process temperature above specification • Sensor error • Error in sensor connection
2	ERR_SENSOR_TEMP_UNDER_RANGE	Possible causes: • Process temperature below specification • Sensor error • Error in sensor connection
3	ERR_SENSOR	Possible causes: • Error in sensor connection • Internal error
4	ERR_CJ	Possible causes: • Cj temperature to high • Cj temperature to low • Cj error
5	ERR_INTERNAL	Internal error
6	ERR_INTERNAL	Internal error
7	ERR_INTERNAL	Internal error
8	Reserved	
9	Reserved	
10	Reserved	
11	Reserved	
12	Reserved	
13	Reserved	
14	Reserved	
15	Reserved	

Pentronic AB
Bergsliden 1
SE-593 96 Västervik
Sweden
Tel.: +46 490-25 85 00
www.pentronic.se
info@pentronic.se