SIL Safety Manual

PLB5000 Temperature Gateway

PLG5465

Rev 2

Pentronic AB
Bergsliden 1
SE-593 96 Västervik
Sweden

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

Contents

List of Figures

List of Tables

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 PLG5465 gateway and the revision of this document. To locate the product revision of the gateway see section 3.1.

Table 1.1: Document history

Document revision	Release date	Revision notes	Product revision
1 (56547)	2019-10-25	First release	1.0.X
2 (79812)	2026-08-17	Updated supply voltage	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 PLG5465 gateway. The recommendations and requirements in this manual shall be considered and implemented during, installation, commissioning, operation and decommissioning of the gateway.

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 = 1×10^{-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 PLG5465 gateway. 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
PLG5465 User manual
PLG5465 Ex Safety instructions
PLG5465 Data sheet

The PLG5465 gateway 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 electro-magnetic 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

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 sys-tems
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
IEC 61326-3-1:2008	Electrical equipment for measurement, control and laboratory use - EMC requirements- Part 3-1: Immunity requirements for safety-related systems and for equipment intended to per-form safety-related functions (functional safety) - General industrial applications
EN 55011:2009	Industrial, scientific and medical equipment - Radio frequency disturbance char-acteristics - Limits and methods of measurement with amendment EN 55011:2009/A1:2010
IEC 60079-0:2017	Explosive atmospheres – Part 0: Equipment – General requirements
IEC 60079-7:2015	Explosive atmospheres – Part 7: Equipment protection by increased safety ”e”

3 Product description

The PLG5465 gateway is a gateway between PLB5000 temperature transmitters and a functional safety PLC. A PLB5000 measurement system may contain up to 120 transmitter measurement channels connected to a gateway. The transmitters and gateway are connected via the PLB BUS, and a secure and very robust safety protocol is used for the communication between the gateway and transmitters. The gateway monitors and collects temperature values from the transmitters and propagates them via the PROFIsafe protocol which is superimposed on the standard PROFIBUS DPV1 protocol to a PLC.

The gateway is qualified to be a part of a SIL2 Safety Instrumented Function (SIF) operating in high, continuous or low demand mode.

Via a web interface the number of transmitters, the order of the temperatures sent to the PLC as well as PROFIsafe and PROFIBUS parameters are configurable. The configuration interface is disabled when the PROFIsafe communication is activated in the gateway, thus making undesired configuration changes impossible.

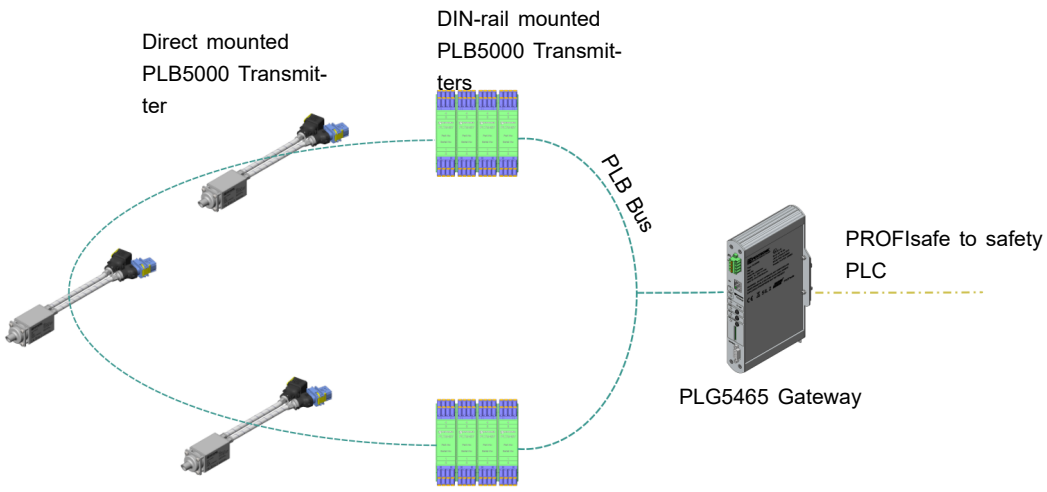

Figure 3.1: PLB5000 measurement system

3.1 Product marking

Information regarding product revision, supply voltage etc is located on the side of the gateway, see figure 3.2.
NOTE! For more information regarding the EX marking and installation in EX zone consult the *PLG5465 Ex Safety instructions*.

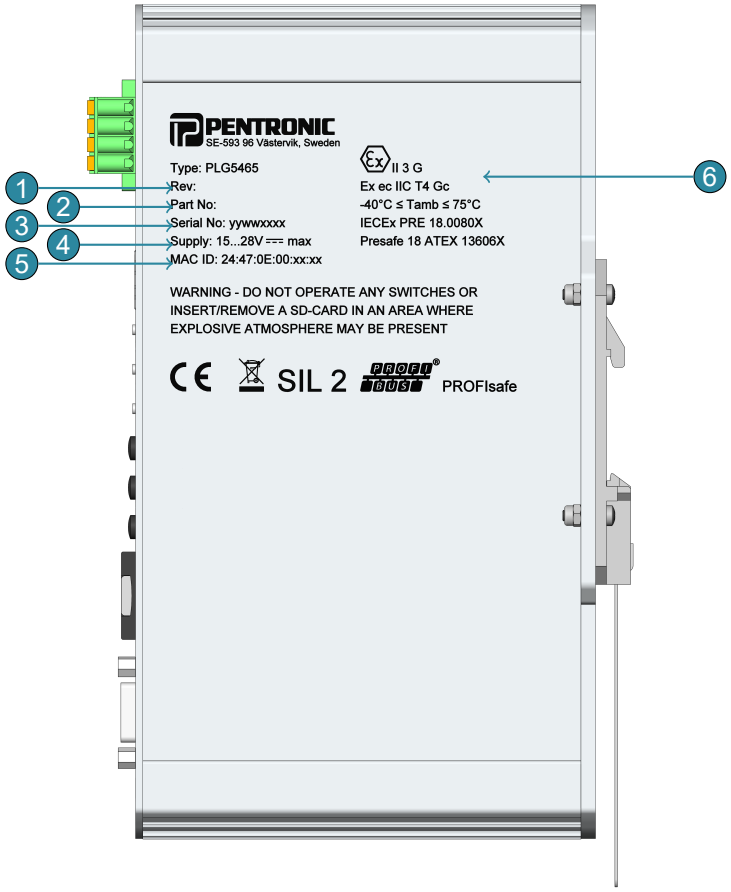

Figure 3.2: Product marking of the PLG5465 gateway

1. Product revision of gateway
   NOTE! Verify that the revision of this safety manual correlates with the revision on the product (see table 1.1)
2. Part number
3. Serial number
4. Rated supply voltage
5. MAC address for Ethernet configuration port
6. EX-marking

4 Installation

The gateway shall be installed on a standard 35 mm DIN rail. The gateway shall be grounded via the DIN-rail mount by external equipotential bonding. If the gateway shall be used in potentially explosive areas please consult the *PLG5465 Ex Safety instructions*.

4.1 Constraints and limitations for use

The gateway has an ingress protection of IP20 and the ambient temperature during operation shall be between -40 and +75 C°. It is the responsibility of the designer of the SIF to verify that the gateway complies with the expected environmental limits and ensure that ambient temperature of the application is within these limits. For more information regarding technical specification consult the *PLG5465 User manual*.

5 | Configuration

To ensure that the configuration of the gateway is not altered by mistake or negligence, the configuration interface is disabled when the PROFIBUS interface is enabled. To enable/disable the interfaces see 5.1.

NOTE! Ensure that only authorized personnel have access to the PLG5465 gateway.

5.1 Safety LED and Safety/Configuration button

By pressing and holding the Safety/Configuration button Q during power-up, the configuration or PROFIBUS interface is either enabled or disabled as indicated by the safety LED I (see table 5.1).

Table 5.1: Safety LED

LED Color	Definition
Green	Safety mode enabled
Red	Configuration mode enabled

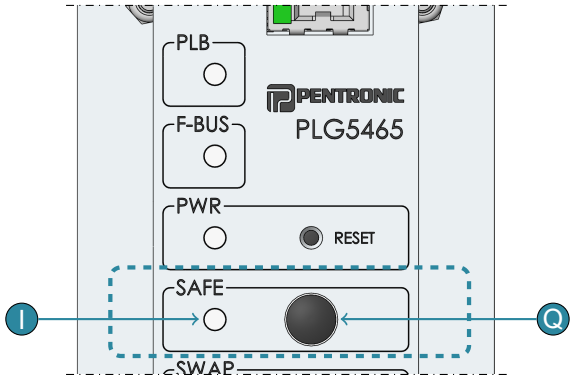

Figure 5.1: Safety/Configuration mode button and Safety LED

5.2 Web configuration Interface

The PLG5465 gateway is configured via a web site, accessible via the Ethernet port (see figure 5.2) on the front panel.

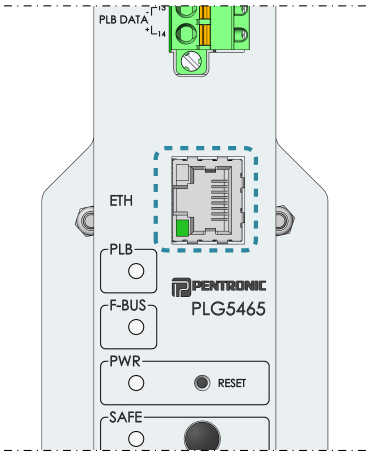

Figure 5.2: Configuration port location

The IP address of the configuration interfaces is static and the default address is **192.168.0.10** (to change the IP address see section 5.2.3 *Ethernet settings*).

Connect the Ethernet port to a PC and enter the IP address to the gateway in a web browser. The *OVERVIEW* page will be displayed, see figure 5.3. For configuration choose either *FIELDBUS SETTINGS*, *FIELDBUS DATA* or *ETHERNET SETTINGS*, see section 5.2.1, 5.2.2 or 5.2.3.

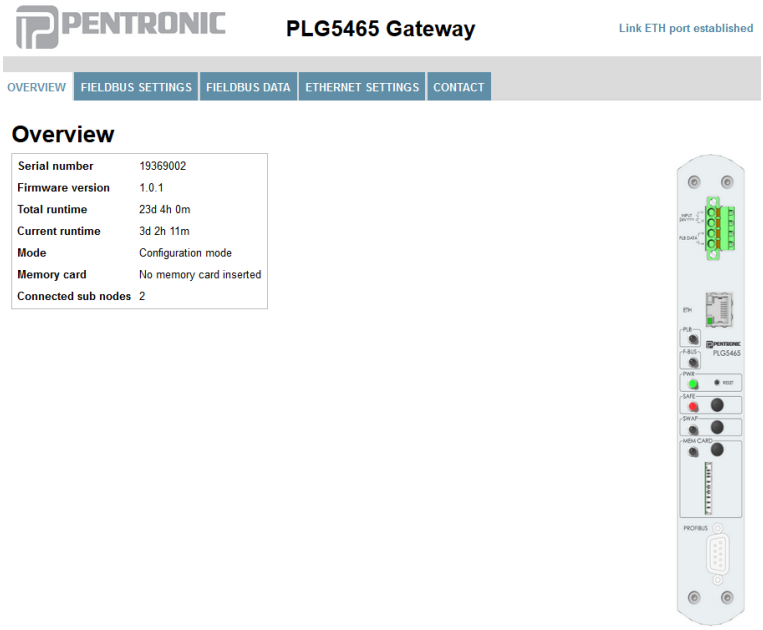

Figure 5.3: Overview web page

5.2.1 Fieldbus settings

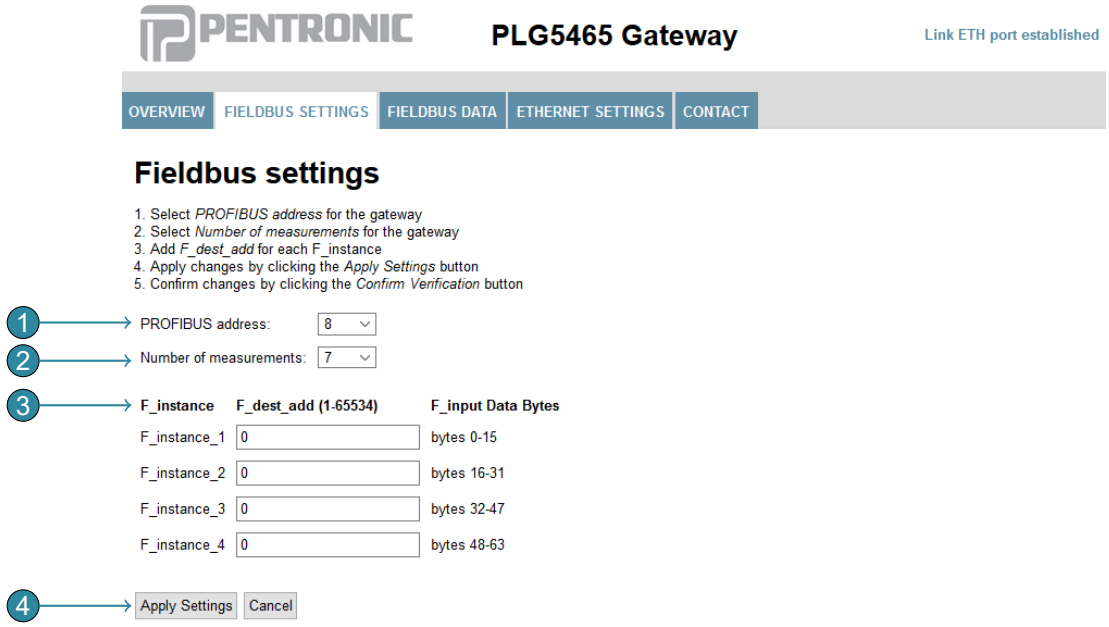

Figure 5.4: Configuration of fieldbus settings

1. The PROFIBUS address of the gateway, a value between 1…125.
   Ensure that the address of the gateway corresponds to the address configured in the PLC.
2. The number of transmitter measurement channels that will be connected to the gateway, a value between 1…120.
3. The number of *F_instances* is dependent of the number of measurements selected in 2 and is calculated by the web page. Each *F_instance* needs a unique *F_dest_add*, a value between 1…65534. The *F_input Data bytes* is the byte offset for the *F_instance* in the PROFIBUS message.
   Ensure that the number of *F_instances* and their *F_dest_add* corresponds with the settings made in the PLC.
4. Saves the configuration and restarts the gateway.

NOTE! When the gateway has restarted, the correctness of the altered configuration shall be verified by the user.

5.2.2 Fieldbus data

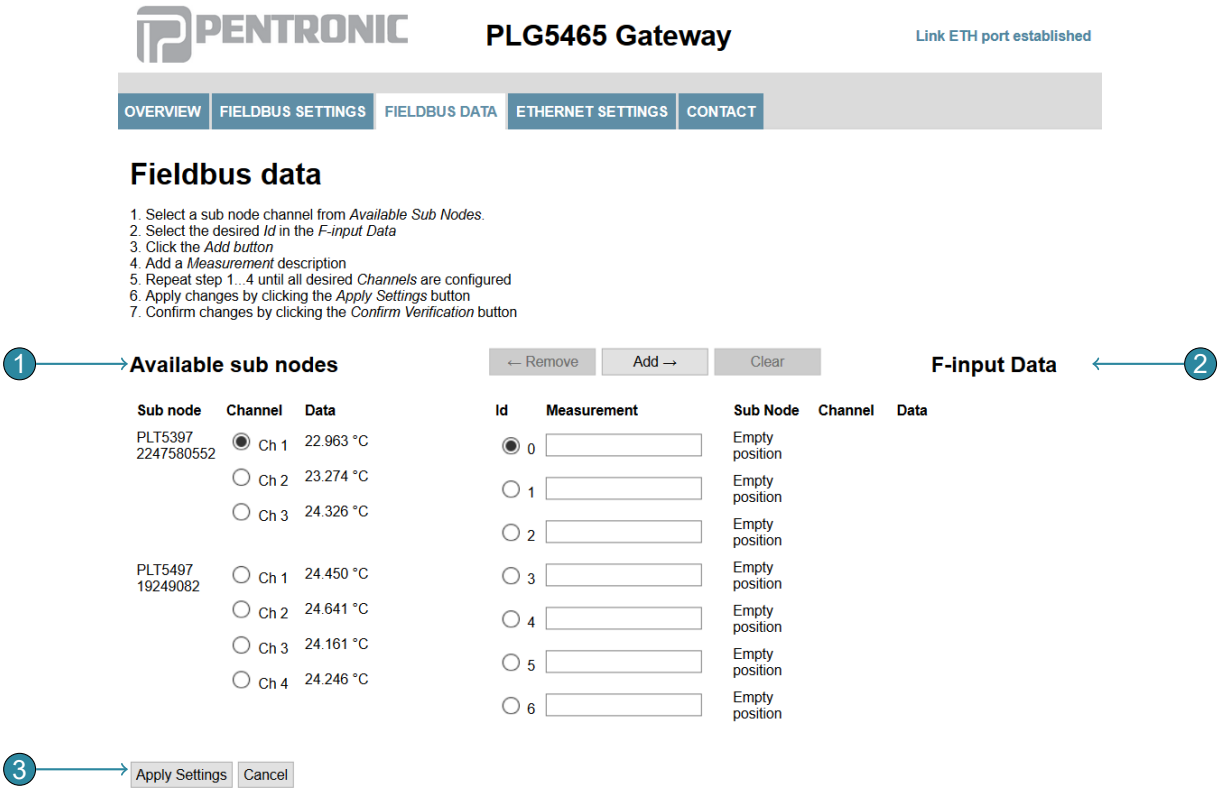

Figure 5.5: Configuration of fieldbus data

1. Connected transmitters will appear in the list *Available sub nodes*. To add a measurement channel from a transmitter to the *F-input data* (the data sent to the PLC), click on the desired channel in the list.
2. When selecting an *Id* (position) in the *F-input Data* for the channel selected in 1, a describing text may also be added for the *Id*. By clicking the **Add** button, the selected channel in 1 will be added to the selected **Id** in **F-input data**.
3. Saves the configuration and restarts the gateway.
   NOTE! When the gateway has restarted, the correctness of the altered configuration shall be verified by the user.

5.2.3 Ethernet settings

The default IP address of the configuration interface is **192.168.0.10**. The *IP address*, *Subnet Mask* and the *Gateway Address* for the configuration interface may be changed via the *ETHERNET SETTINGS* web page see figure 5.6.

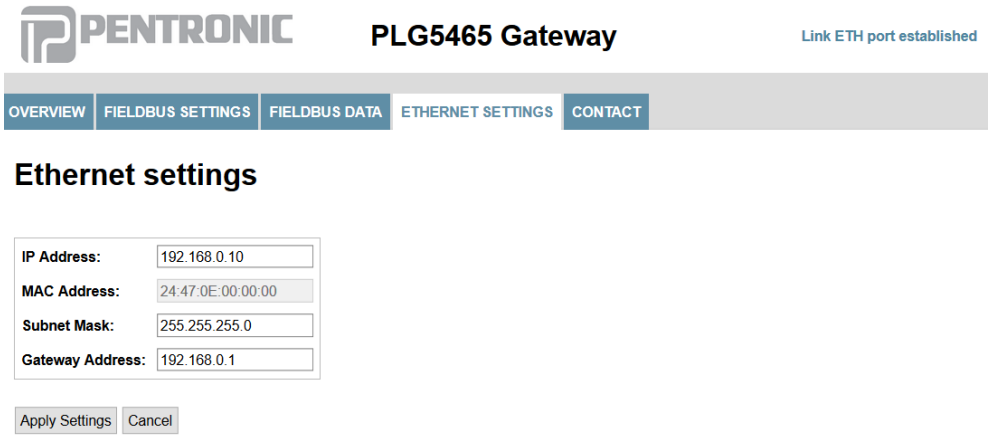

Figure 5.6: Ethernet settings for configuration interface

6 PROFIBUS interface

6.1 PROFIBUS termination

The PLG5465 gateway has no built in termination resistance for PROFIBUS. If the bus topology requires that the PLG5465 PROFIBUS node shall be terminated, use a 9 pin sub-D with built in termination circuitry. For further details, consult the *PROFIBUS Design Guideline, Version 1.13, Order No: 8.012* or later.

6.2 PROFIBUS address

See section 5.2.1 *Fieldbus settings*

6.3 PROFIsafe address

See section 5.2.1 *Fieldbus settings*.

6.4 PROFIBUS baud rate

The PROFIBUS baud rate is detected automatically, for supported baud rates see table 6.1.

Table 6.1: Supported PROFIBUS baudrates

Baud rate (kb/s)	Baud rate (Mb/s)
9.6	1.5
19.2	3
45.45	6
93.75	12
187.5	
500	

6.4.1 GSD file

For PROFIBUS, the characteristic features of a device are stored in an ASCII device data file with the suffix GSD. GSD files are used by PROFIBUS configuration tools when setting up a network. The installation procedure of the PLG5465 GSD file depends on the PROFIBUS configuration software; please consult your specific software manual.

6.5 PROFIBUS communication

When the gateway is in DDLM_Data_Exchange mode (i.e cyclic data transfer), temperature values from configured channels (see section 5.2.2 *Fieldbus data*) are sent to the PLC via the PROFIsafe protocol in a PROFIBUS message.

6.5.1 PROFIsafe input data

The gateway can be configured to deliver 1…15 F-instances cyclically, depending of the *Number of measurements* selected in *Fieldbus* web page (see section 5.2.2 *Fieldbus data*). Each F-instance is composed of 16 bytes, see table 6.2.

NOTE! For more information regarding the PROFIsafe protocol, consult the *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, Ver 2.4, Order No: 3.192b*.

Table 6.2: F-instance message

Data	Size	Description
F-Input	12	See table 6.3
Status Byte	1	See *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, Ver 2.4, Order No: 3.192b* for definition
CRC signature	3	See *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, Ver 2.4, Order No: 3.192b* for definition

The F-Input part of the F_instance contains measurement channel data for two measurement channels: channel ”N” and channel ”M” (see table 6.3). ”N” and ”M” corresponds to the positions (*Id*) selected for the channels during configuration, see section 5.2.2 *Fieldbus data*.

The data for one measurement channel consists of four parts:

- **ID_X**: Measurement Id
- **INFO_X**: Indicates if the value for the measurement Id is an temperature or error code
- **DATA_X_I**: Integer part of measurement value or error code from transmitter
- **DATA_X_D**: Decimal part of measurement value or error code from gateway

Table 6.3: F-Input data

	Byte offset	Abbreviation	Description	Data type (*EN 61131-3:2013 Programmable controllers - Part 3: Programming languages*)	Number of octets
F-Input data	0	ID_N	ID number for DATA_N	USINT	1
	1	INFO_N	Information for DATA_N	USINT	1
	2	ID_M	ID number for DATA_M	USINT	1
	3	INFO_M	Information for DATA_M	USINT	1
	4…5	DATA_N_I	Data value N integer part	INT	2
	6…7	DATA_N_D	Data value N decimal part	INT	2
	8…9	DATA_M_I	Data value M integer part	INT	2
	10…11	DATA_M_D	Data value M decimal part	INT	2
F-Trailer	12	Status byte	PROFIsafe status byte for F-instances X	F message trailer with 4 octets	1
	13…15	CRC2	PROFIsafe crc for F-instance X		3

6.5.2 Paging of temperature values

The gateway supports 15 F-instances and each F-instance represents two temperature values, thus 30 temperature values from 30 transmitter channels can be sent in a single PROFIBUS message. The temperature representations will be divided into pages (F_{pages}), see table 6.4, if more than 30 temperature channels are configured.

Table 6.4: Pages for F-Input data

Number of transmitter channels	Number of pages (F_{pages})
1…30	1
31…60	2
61…90	3
91…120	4

See figure 6.1 for an example of F-Input data for a PLG5465 configured with 90 transmitter channels.

Number of configured transmitter channels: $X = 90$

Temperatures / F-instance: $Y = 2$

Number of F-instances: $Z = 15$

Number of pages: $F_{pages} = \frac{X}{Y \times Z} \rightarrow \frac{90}{2 \times 15} = 3$

	F-instance 1		F-instance 2		…		F-instance 15	
Update cycle 1								
F_{pages} = 1	ID = 0	ID =1	ID = 2	ID = 3	…	…	ID = 28	ID = 29
Update cycle 2								
F_{pages} = 2	ID = 30	ID =31	ID = 32	ID = 33	…	…	ID = 58	ID = 59
Update cycle 3								
F_{pages} = 3	ID = 60	ID =61	ID = 62	ID = 63	…	…	ID = 88	ID = 89

Figure 6.1: Example of F-Input update cycle for 90 transmitter channels

6.5.3 Temperature representation

A temperature value is separated in to two parts, DATA_X_I which contains the integer representation, and DATA_X_D, which contains the decimal part (see table 6.3). To obtain a decimal representation of the temperature combine the two values as described by equation 6.1. Table 6.5 contains examples of how different temperature values will be presented in the F-input data.

$$\text{Temperature value } = DATA\_X\_I + \frac{DATA\_X\_D}{2^{14}} \tag{6.1}$$

Table 6.5: Representation of temperature values in F-Input data

Temperature value (decimal)	DATA_X_I	DATA_X_D
+156.0001	156	2
+156.001	156	16
+156.01	156	164
+156.1	156	1638
-156.1234	-156	-2022
-0.0001	0	-2

6.5.4 Error code representation

If a configured transmitter is unable to deliver a safe temperature value for its measurement channel due to an erroneous condition, or if the gateway detects an error for the configured transmitter, the temperature value in F-Input data will be replaced with a corresponding error code.

If an error has occurred for a configured transmitter channel, BIT7 in the corresponding INFO_X byte (see table 6.3) will be set to 1. If the error is of a type detected by the transmitter, the data in DATA_X_I will be replaced with an error code. If the error is detected by gateway, the value in DATA_X_D will be replaced by an error code, see table 6.6.

Table 6.6: Error representation in F-Input data

BIT	Abbreviation	Value	Description
0	INFO_X	…	Reserved
1		…	Reserved
2		…	Reserved
3		…	Reserved
4		…	Reserved
5		…	Reserved
6		…	Reserved
7		1	BIT7 will be set to 1 in case of an error code
	DATA_X_I		Contains the corresponding transmitter error code
	DATA_X_D		Contains the corresponding gateway error code

6.5.5 Gateway error codes

Table 6.7: Gateway error codes in DATA_X_D

BIT	DECIMAL	Abbreviation	Error Description
0	1	ERR_UNCONFIGURED_POSITION	No transmitter channel configured for this position
1	2	ERR_BUS	Possible causes: • Bus cable short circuit
2	4	ERR_NO_RESPONSE	Possible causes: • Transmitter disconnected • Transmitter powered off • Erroneous transmitter
3	8	ERR_SUB_NODE_INTERNAL	Transmitter malfunction
4	16	ERR_SAFE_VALS_ACTIVATED	The PLC has activated the BIT *activate_FV_C* in the Control byte for the F-Trailer*
5	32	Reserved	
6	64	Reserved	
7	128	Reserved	
8	256	Reserved	
9	512	Reserved	
10	1024	Reserved	
11	2048	Reserved	
12	4096	Reserved	
13	8192	Reserved	
14	16384	Reserved	
15	32768	Reserved	

* For more information regarding the PROFIsafe Control byte, sent from the PLC consult the document *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, Ver 2.4, Order No: 3.192b*

6.5.6 Transmitter error codes

For transmitter error codes in DATA_X_I, please consult the transmitter documentation.

6.6 PROFIsafe output data

F_Output data is not supported for PLG5465. In data exchange the PLC sends the mandatory F_Trailer part (see table 6.8) of the PROFIsafe message for each configured F-instance to the PLG5465 gateway.

NOTE! For more information regarding F_Trailer consult the document *PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO, Ver 2.4, Order No: 3.192b*.

Table 6.8: F-Output data signal list

	Byte offset	Abbreviation	Description	Data type (*EN 61131-3:2013 Programmable controllers - Part 3: Programming languages*)	Number of octets
F-Trailer	0	Control byte	PROFIsafe control byte for F-instances X	F message trailer with 4 octets	1
	1…3	CRC2	PROFIsafe crc for F-instance X		3

7 Functional test

It is the responsibility of the end user to perform a functional test of the gateway, 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 correct values for all configured transmitter channels are present in the PLC.

NOTE! For proof test procedure see chapter 13

8 Maintenance

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

9 Notification of failures

In case of malfunction of the gateway, 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 gateway 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.

10 Decommissioning

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

11 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.

11.1 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.

11.2 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.

11.3 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.

11.4 Configuration management

Procedures for configuration management shall be established and used during the whole life cycle of the gateway. 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 gateway product revision).

11.5 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.

12 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 gateway specific safety data see chapter 14.

12.1 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} (undetectable).

12.1.1 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 (PDF$_{avg}$).

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 12.1.

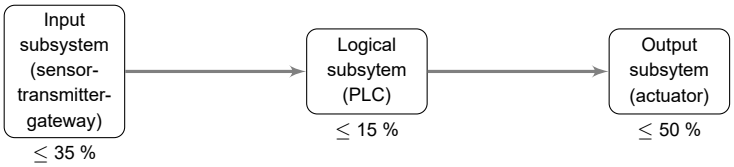

Figure 12.1: Example of PFD$_{avg}$ /PFH distribution in subsystems

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 12.1.

Table 12.1: Correlation between SIL capability and PFD$_{avg}$ and PFH

SIL	PDF$_{avg}$	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.

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

12.1.2 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.

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

12.2 Architectural constraints

According to IEC 61508 there are two possible routes to fullfill 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).

12.2.1 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.

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

12.2.2 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 12.2 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 12.2: 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

12.3 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 n 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.

13 | 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 gateway 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 gateway.

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 gateway 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 9).

13.1 Proof test procedure

A recommended proof test procedure is described below. This test will detect 92% of possible λ_{DU} failures in the gateway.

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

13.1.1 Test case 1

1. Bypass the safety function and take appropriate action to avoid a false trip.
2. Verify that the values from the transmitters are as expected in the PLC.
3. Disconnect a transmitter and verify that an error code is present for the disconnected transmitter in the PLC.
4. Reconnect the transmitter and verify that the error code is replaced with the expected temperature value.

13.1.2 Test case 2

1. Bypass the safety function and take appropriate action to avoid a false trip.
2. Enable the configuration interface of the gateway
3. Verify that the gateway configuration is correct

13.1.3 Test case 3

1. Bypass the safety function and take appropriate action to avoid a false trip.
2. Power off the gateway.
3. Disconnect the transmitters from the gateway.
4. Connect a multimeter to *PLB DATA+* and *PLB DATA-* (1).
5. Press and hold the reset button (2).
6. Turn power on while keeping the reset button prest.
7. Measure the output voltage on *PLB DATA*, the maximum voltage measured shall be $\geq$ 4.1 VDC.
8. Release reset button

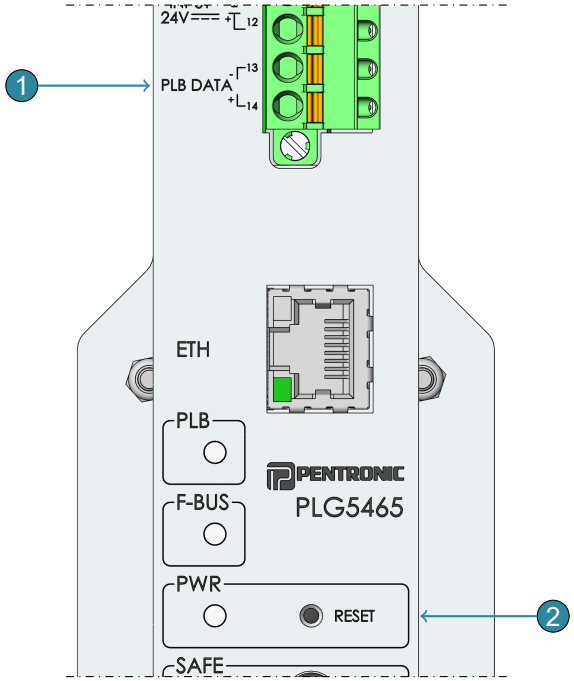

Figure 13.1: PLB supply voltage measurement

14 Device specific safety information

14.1 SIL certification

RISE - Research Institutes of Sweden has performed an full assessment of the PLG5465 gateway against all applicable requirements in IEC 61508:2010 and the gateway fullfills:

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

14.2 Safety function

The gateway monitors and collects temperature values from PLB5000 temperature transmitters and provides the measurement values or error codes on the PROFIsafe interface to a safety PLC.

14.3 Fault detection and reaction time (FDTR)

If the internal diagnostics in the gateway detects an error (λ_{DD}), the gateway will enter safe state. The maximum fault detection and reaction time (FDTR) is less than 10 seconds. The gateway will stay in safe state until the error is resolved, for more information regarding error codes see section 6.5.5 and 6.5.6. 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 gateway may deliver incorrect transmitter data.

NOTE! If the gateway is restarted and the error condition still persists it may take up to: start up time (20s) + FDTR (<10s) before safe state is entered.

14.4 Safe state

The gateway 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 safety PLC
2. An error code is provided instead of transmitter data up on request.

14.5 Demand response time

The maximum demand response time is less than 1 second. This is the maximum time from when new transmitter data is received by the gateway, until it is made available for the safety PLC.

14.6 Type classification

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

14.7 Mode of operation

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

If the gateway 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.

14.8 Reliability data

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

Failure rate data listed in table 14.1 are only valid for the useful life time of the gateway, reliability calculations based on the failure rates for the gateway 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 92%.
- Safe failures are regarded as dangerous failures with a diagnostic coverage of 99%
- The device is installed according to manufactures instruction.
- The gateway is a Type B element with a HFT of 0.
- External power supply failures are not considered.
- Ambient temperature 40 °C.

Table 14.1: Reliability data for PLG5465 gateway

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
0	0	785	20	0	58	97.6	97.6	2.0	1.9	2.7	5.0

NOTE! The failure rates for all elements in a SIF shall be considered, hence SFF, PFH, DC and PDF_{avg} values in table 14.1 shall be regarded as reference values only. It is the responsibility of the SIF designer to calculate SFF, PFH, DC and PDF_{avg} values for respectively SIF.

This page intentionally left blank

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