Dräger

Dräger PIR 7000 / Dräger PIR 7200
Infrared Gas Transmitter
Safety Manual

Dräger. Technology for Life®

Content

1 Scope and purpose of safety manual

The purpose of this safety manual is to document the necessary information and assumptions, that are required for the integration of the assessed gas transmitters

- Dräger PIR 7000 and Dräger PIR 7200

into a safety instrumented system (SIS) - in compliance with the requirements of IEC 61508 standard.

The safety manual specifies the safety functions. This may be used to support the safety function of a safety instrumented system (SIS).

The safety manual provides the assumptions that have been made on the usage of the gas transmitter. If those assumptions cannot be met by the application, the SIL capability has to be evaluated considering the application-specific circumstances.

2 Relevant standards

EN 50402:2005 +A1:2008	Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen – requirements on the functional safety of fixed gas detection systems
IEC 61508:2010	Functional safety of electrical / electronic / programmable electronic safety related systems

3 Field of application

The herein considered instruments Dräger PIR 7000 and Dräger PIR 7200 are explosion proof infrared gas transmitters for stationary, continuous monitoring of gases and vapours in a suitable atmosphere.

The Dräger PIR 7000 gas transmitter monitors the concentration of combustible gases and vapours containing hydrocarbons.

The Dräger PIR 7200 gas transmitter monitors the concentration of carbon dioxide.

The gas transmitter uses microprocessor technology to convert the signal measured by the build-in detector components to both a 4 to 20 mA analogue signal output and a serial digital output signal, and a HART® signal (if built-in, optional).

The double-compensating and non-imaging optics effectively compensates for temperature and ageing effects.

The gas transmitter is designed for one-man calibration and offers a variety of diagnostics and self test features.

Different measured gases are listed in an internal gases library. For all these gases, an individual linearisation of the output signal corresponding to the measured gas concentration is provided.

Configuration and calibration are menu guided and easy to perform, using a HART® handheld terminal or a PC (configuration tool).

The safety manual is referring to the following models of Dräger PIR 7000 and Dräger PIR 7200:

Software: Release 1.0, 1.1, 1.2 and Release 2.0.x

Model	Part no.
Dräger PIR 7000 Type 334 (M25) HART	68 11 550
Dräger PIR 7000 Type 334 (M25)	68 11 820
Dräger PIR 7000 Type 334 (NPT) HART	68 11 552
Dräger PIR 7000 Type 334 (NPT) CCCF	68 12 502
Dräger PIR 7000 Type 334 (NPT)	68 11 822
Dräger PIR 7000 Type 334 (M25) HART cpl. Set	68 11 817
Dräger PIR 7000 Type 334 (M25) cpl. Set CCCF	68 12 503
Dräger PIR 7000 Type 334 (M25) cpl. Set	68 11 825
Dräger PIR 7000 Type 334 (NPT) HART cpl. Set SS 316	68 13 035
Dräger PIR 7000 Type 334 (NPT) HART cpl. Set Alu	68 13 030
Dräger PIR 7000 Type 340 (M25) HART	68 11 560
Dräger PIR 7000 Type 340 (M25)	68 11 830
Dräger PIR 7000 Type 340 (NPT) HART	68 11 562
Dräger PIR 7000 Type 340 (NPT)	68 11 832
Dräger PIR 7000 Type 340 (M25) HART cpl. Set	68 11 819
Dräger PIR 7000 Type 340 (NPT) HART cpl. Set SS 316	68 13 045
Dräger PIR 7000 Type 340 (NPT) HART cpl. Set Alu	68 13 040
Dräger PIR 7200 (M25) HART	68 11 570
Dräger PIR 7200 (NPT) HART	68 11 572
Dräger PIR 7200 (M25) HART cpl. Set	68 12 290
Dräger PIR 7200 (NPT) HART cpl. Set SS 316	68 13 055
Dräger PIR 7200 (NPT) HART cpl. Set Alu	68 13 050

4 Assumptions and restrictions for usage of the gas transmitter

4.1 General

For proper installation, operation, maintenance and calibration of the gas transmitter and its accessories strictly follow the Instructions for Use as well as the Installation Instructions for Accessories.

See Instructions for Use for information about assembly and functional description, operating conditions and interface specification.

4.2 Trainings

For available trainings contact DrägerService® [1].

4.3 Installation

The parameterization of the gas transmitter must be checked after installation by reading back the parameters (e.g. with the PC software Dräger PolySoft). Also a calibration and a proof test have to be executed. The user has to ensure that the requirements regarding supply voltage and power consumption, as well as the 4 to 20 mA loop requirements are within the specified range.

The accuracy of gas measurement is depending on ambient parameters. See Instructions for Use for details and measuring performance.

4.4 Maintenance

The reason for repeated maintenance of the gas transmitter is to ensure the safety function of the instrument. Therefore the functionality, the calibration and the parameterisation of the gas transmitter has to be checked at regular intervals. The maintenance interval should not exceed one year.

4.5 Calibration

For calibration ensure that only approved and certified calibration gas is used in accordance with the internal parameterisation of the gas transmitter.

If the deviation of the calibration result is outside the corresponding limits listed in the Instructions for Use, paragraph Calibration (display of the zero-point deviation or display of the sensitivity deviation) the following actions are recommended to be performed:

- Check if the optical surface areas have not been contaminated.
- Check the leak tightness of the calibration equipment.
- Ensure proper calibration gas flow.
- Rerun the calibration.

See Instructions for Use for calibration procedure.

4.6 Replacement

If a gas transmitter needs to be replaced (for repair or exchange), the parameterisation of the replacing gas transmitter must be checked. A calibration and a proof test have to be executed. The time assumed for replacement is 8 hours.

CAUTION

Check if the replacing gas transmitter is locked for unauthorised access to calibration and/or configuration (SIL lock), if not: lock it.

4.7 Hardware configuration

The gas transmitter is configurable over a wide range of settings. If any setting is changed the parameters must be confirmed by authorized personnel. In case of using a configuration tool, check all parameters listed on the confirmation screen. To confirm the parameter the gas transmitter has to be locked into the SIL mode.

CAUTION

The usage of the HART® signal and the usage of the serial digital output signal is only allowed if the safety instrumented application supports the "Read Safe Digital Measurement Value" and fulfills the requirements described in Chapter 7.2 and IEC 61508.

4.8 Use of accessories

Use only original Dräger PIR 7000 and Dräger PIR 7200 accessories. Part nos. see Instructions for Use, descriptions see specific Installation instructions.

4.9 Access rights option

Three levels of access rights and related user groups of different qualification are distinguished.

- Operator – should not get any tool (Magnetic Wand, PC software Dräger PolySoft and tools to communicate by the HART® interface) to unlock the gas transmitter for calibration or configuration.
- Calibration personnel – has the Dräger Magnetic Wand to unlock the gas transmitter for calibration purposes and to lock it again after successful calibration.
- Parameterisation personnel – has the password and a tool to unlock the gas transmitter for modification and parameterisation of safety-related parameters.

CAUTION

Locking of the gas transmitter is required for SIL operation, i.e. an unlocked gas transmitter may not be used in SIL applications.

1 DrägerService® is a registered trade mark from Dräger.

5 Proof test

All safety related data are based on repeated proof tests performed at regular intervals, provided that the proof tests have been successful.

Proof testing is an essential part of functional safety because this is the only way to detect unrevealed dangerous failures. The compliance with these proof test intervals is under the responsibility of the user of the safety equipment.

During the proof test the functional safety is affected and must be ensured by other measures, also organisational measures, or the safety instrumented system (SIS) needs to be forced and maintained in a safe state.

NOTICE

Not only the gas transmitter needs to be tested, but the safety function of the whole safety instrumented system (SIS).

The proof test consists of the following steps:

Steps for proof test to be passed

Step	Action
1	Take appropriate actions to avoid any dangerous action of the safety -instrumented system (SIS) during the proof test.
2	Check all the accessories in use (e.g. Splash Guard, Insect Guard, Hydrophobic Filter) for contamination or damage. Clean or replace these accessories if necessary.
3	Check the gas transmitter's optical surface areas for contamination. If contaminated, clean and dry these areas (see Instructions for Use).
4	Perform zero-point calibration and span calibration.
5	Test for proper fault condition indication of the transmitter by ● either blocking the optical path, or ● sending a digital command to set the current output of the transmitter to fault condition. Make sure the safety instrumented system (SIS) recognizes fault condition state.
6	Apply zero test gas, check if the safety instrumented system (SIS) displays the -expected value.
7	Apply a test gas of an adequate concentration to trigger the alarm -thresholds being used in the safety instrumented system (SIS). Make sure the safety instrumented system (SIS) recognizes alarm condition.
8	Restore the standard operating mode.

6 Safety relevant parameters

Parameter	Description
Measured gas	Selected measured gas (e.g. "Methane").
Measurement unit	Selected unit (e.g. "%LEL").
Measuring range	Gas concentration in the configured measured gas unit which will lead to an output signal of 20 mA on the 4 to 20 mA interface.
LEL category	Five categories available: 1: "NIOSH", 2: "IEC", 3: "PTB", 4: "RUS", 5: "LKLV".
LEL of measured gas / calibration gas	Gas concentration in ppm where the Lower Explosion Limit (LEL) is 100%, depending on national or regional regulations.
Capture value and limits	Clamping the signal output to the capture value for measurement readings within the capture value limits.
Calibration gas	Selected calibration gas (e.g. "Methane").
Calibration gas unit	Selected unit for calibration gas concentration (e.g. "Vol.%").
Calibration gas - concentration	Concentration of calibration gas. The user has to check the parameter against labelling of the calibration gas cylinder.
Zero-point parameters	See Instructions for Use, Calibration
Span parameters	See Instructions for Use, Calibration

NOTICE

Refer to the Instructions for Use for further information.

7 Functional specifications of the safety functions

Measure the concentration of hydrocarbons and carbon dioxide in the atmosphere by absorbing infrared radiation and set the 4 to 20 mA output accordingly or provide the measurement value via HART® signal or serial digital output signal (ICOM).

Definition Fail Dangerous: Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or results in an output measurement value which is:

- 10 % below the measured gas concentration or
- 3 % of full scale below the measured gas concentration whichever is the greater.

The deviation between measured value and true concentration can exceed above errors.

NOTICE

For detailed information see chapter “Technical data” in the Instructions for Use.

7.1 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the infrared gas transmitter Dräger PIR 7000 and Dräger PIR 7200.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Materials are compatible with process conditions.
- The instrument is locked against unintended operation/ modification.
- External power supply failure rates are not included.
- The meantime to restoration (MTTR) after a safe failure is 8 hours.
- The test time of a connected safety PLC to react on a dangerous detected failure and bring the process to the safe state is 1 hour.
- The listed failure rates are valid for operating stress conditions typical of an industrial environment similar to IEC 60654-1 class C (sheltered location) with temperature limits within the manufacturer’s rating and an average temperature over a long period of time of 40 °C (25 °C ambient temperature plus internal self heating). For higher average temperatures, the failure rates should be multiplied with an experience based factor of e.g. 1.5 for 50°C , 2.5 for 60 °C and 5 for 80°C. A factor of 2.5 should be used if frequent temperature fluctuation (daily fluctuation of > 15 °C) must be assumed. Humidity levels are assumed within manufacturer’s rating.
- Only the described versions are used for safety applications.
- The 4 to 20 mA output signal is fed to a SIL 2 compliant analogue input board of a safety SIS.
- When using the 4 to 20 mA output signal the application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- General necessary gas detection tests have successfully been passed.

7.2 4 to 20 mA current output

The entire valid measurement range for the output signal is between min. 3.8 mA and max. 20.5 mA.

Fault, maintenance and beam block warning signal may be configured as follows:

Current [mA]	Meaning	Configurable (0.7 … 3.6 mA)
< 1.2	Fault (including memory error and runtime error)	Yes
3.0	Maintenance	Yes
2.0	Beam block warning	Yes
> 21	Defect in analogue interface	---

CAUTION

The user must ensure the configuration of different current levels for the above listed signals.

NOTICE

For detailed information see chapter “Configuration of the 4...20 mA current output” in the Instructions for Use.

7.3 Safe Digital Measurement Value via HART® and ICOM

The gas transmitters Dräger PIR 7000 and Dräger PIR 7200 provide a serial interface for a safe bus communication via HART® signal (HART) or serial digital output signal (ICOM).

The “black channel” principle shall be used for that safety related data communication. It means to transport safety related data over a non-safe channel.

The measurement value is secured and transported via a master-slave communication from the Dräger PIR 7x00 via HART/ICOM to the safety instrumented system (SIS).

The data integrity is ensured by the measures CRC and time stamp.

NOTICE

With the “black channel” mechanism sender and receiver can check the correctness of the message (verify the reliability of the data) on a non-safe bus communication. This is done at Dräger on base of the faults assumptions of the standard IEC 61784-3:2010. This is sufficient for SIL 2 requirements according to IEC 61508.

WARNING

The safety instrumented system (SIS) shall support the “Read Safe Digital Measurement Value” (command ID: 129 / see for details chapter 7.2.2). The Dräger PIR 7x00 is implemented as slave in the communication with the safety instrumented system (SIS) whereas the SIS has to be the master in the bus communication.

The safety instrumented system (SIS) has to fulfill all requirements according to SIL 2 or higher [Standard IEC 61508:2010 or EN 50402:2005 + A1:2008].

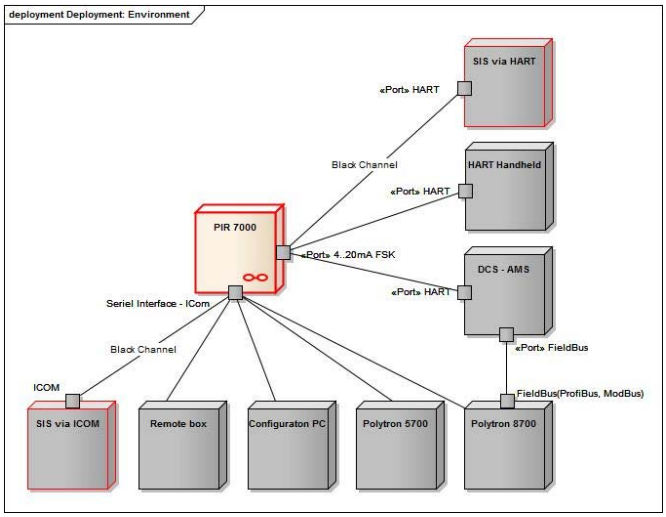
7.3.1 Integration into a SIS

In this chapter it is explained how the Dräger PIR 7x00 has to be integrated into a safety instrumented system (SIS). The following connections are possible:

HART® can be connected to a SIS and a HART® Handheld Terminal (HHT).

ICOM can be connected only to one device at a time (e.g. SIS).

Configuration of the IR Gas Transmitter Dräger PIR 7x00 variants:



7.3.2 Requirements for safety instrumented system (Master)

The following requirements have to be fulfilled by the master in order to make use of the black channel principle and use the master-slave communication for the Dräger PIR 7x00 and the functionality for reading a safe digital measurement value.

The following naming convention is used:

Request: Master to Dräger PIR 7x00

Response: Dräger PIR 7x00 to Master

NOTICE

To improve the reliability of access in multidrop control systems any HART master must issue a unique polling address to each member of the driven line.

It is mandatory to confirm these Polling Addresses after configuration.

The master must send a safe request.

Safe request:

This is what the master has to fulfill before sending a valid request:

- The master has to provide a CRC[1].
- The master must issue any request with a unique time stamp that is increased for each message.
- In a multidrop installation the master must issue the request with the polling address set and with "Check Poll.Addr" enabled.

Safe response:

The master must maintain a watch dog functionality to detect missing responses. The time out time of the master shall be 256 ms.

Following the master has to check after receiving a safe response from PIR before using the measurement value:

- The master must check the CRC.
- The master must verify the received time stamp with the issued one.

Request Data Bytes

Byte	Format	Descript.
0...3	U32	CRC32
4	U8	0x80 : 0 0x40 : 0 0x20 : 0 0x10 : 0 0x08 - 0x01 : Version of safe Protocol
5	U8	0x80 : Check Polling Address enabled 0x40 : 0 0x20 : 0 0x10 : 0 0x08 - 0x01 : Polling address (<=15!)
6...9	U32	Time Stamp

Response Data Bytes

Byte	Format	Descript.
0...3	U32	CRC32
4	U8	0x80 : 0 0x40 : 0 0x20 : 0 0x10 : 0 0x08 - 0x01 : 1 (actual version of safe protocol)
5	U8	0x80 : Check Polling Address enabled 0x40 : 0 0x20 : 0 0x10 : 0 0x08 - 0x01 : Polling address
6...9	U32	Time Stamp
10	U8	reserved
11	U8	Reserved
12...15	F32	Measurement Value in configured Unit

Command Specific Response Codes

Code	Description
0	No Command-Specific Errors

U8: unsigned integer 8 Bit
U32: unsigned integer 32 Bit little endian
F32: floating point IEEE754

7.3.3 Possible failures and their causes

Fault assumption	Possible causes
Dräger PIR 7x00 does not respond	Wrong request because of: Frame defect CRC32 Polling address Master time out wrong (<256ms) No electrical contact
Dräger PIR 7x00's response contains wrong [corrupt data]	Bus communication disturbed
Dräger PIR 7x00 does not answer to every request	Master sends too many requests

1 Polynomial = 0xF4ACFB13.Size = 32 bit, Seed = 0xFFFFFFFF, ReflectIn = enable, ReflectOut = enable, FinalXOR = 0xFFFFFFFF

7.4 Parameters related to the above safety function

Diagnostic test interval	≤ 2 seconds
Diagnostic test interval (memory test)	≤ 6.5 hours
Hardware Fault Tolerance (HFT)	0
Component type	Type B
SIL capability	SIL 2
Description of the safe state For safe digital measurement value: No Response within time or error flag set and measurement value is NaN (not a number)	Configured alarm ≤ 3.6 mA
Architecture	1oo1
MTBF	105 years
Useful lifetime (maximum)	12 years
Measured value response time	See Instructions for Use

7.4.1 Useful lifetime

Although a constant failure rate is assumed by the probabilistic estimation method this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions, especially its temperature.

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component. The experience based useful lifetime is usually between 8 and 12 years. (IEC 61508-2, 7.4.9.5, Remark 3)

7.4.2 Operation in current source mode

Failure category	Failure rates (in FIT)
λ_{SD} Fail safe detected	0
λ_{SU} Fail safe undetected	9
λ_{DD} Fail dangerous detected	692
λ_{DU} Fail dangerous undetected	49

Safe failure fraction (SFF)	93 %
DC_D	93 %

PFD_{AVG} (T[Proof] = 1 year)	2.39E-04
PFD_{AVG} (T[Proof] = 5 years)	1.09E-03
PFD_{AVG} (T[Proof] = 10 years)	2.15E-03
PFH	4.89E-08 1/h

7.4.3 Operation in current sink mode

Failure category	Failure rates (in FIT)
λ_{SD} Fail safe detected	0
λ_{SU} Fail safe undetected	0
λ_{DD} Fail dangerous detected	640
λ_{DU} Fail dangerous undetected	70

Safe failure fraction (SFF)	90 %
DC_D	90 %

PFD_{AVG} (T[Proof] = 1 year)	3.39E-04
PFD_{AVG} (T[Proof] = 5 years)	1.55E-03
PFD_{AVG} (T[Proof] = 10 years])	3.07E-03
PFH	7.00E-08 1/h

7.4.4 Operation in HART®/ICOM mode

For simultaneous usage of digital communication (HART®/ ICOM) and analog communication use of the values for pure analog communication is recommended.

Failure category	Failure rates (in FIT)
λ_{SD} Fail safe detected	0
λ_{SU} Fail safe undetected	126
λ_{DD} Fail dangerous detected	435
λ_{DU} Fail dangerous undetected	43

Safe failure fraction (SFF)	92 %
DC_D	91 %

PFD_{AVG} (T[Proof] = 1 year)	2.08E-04
PFD_{AVG} (T[Proof] = 5 years)	9.50E-04
PFD_{AVG} (T[Proof] = 10 years])	1.88E-03
PFH	4.28E-08 1/h

8 Reference documents

Document	Part no.
Instructions for Use Dräger PIR 7000 / Dräger PIR 7200	90 23 885
Technical Handbook Dräger PIR 7000 / Dräger PIR 7200	90 23 886

9 List of abbreviations

DC_D	Diagnostic Coverage of Dangerous failures ($DC_D = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$)
DU	Dangerous Undetected (failure)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HART®	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
IR	Infrared
Low demand mode	Mode, where the frequency of demands for operation made on a safety instrumented system (SIS) is no greater than one per year and no greater than twice the proof test - frequency.
MTBF	Meantime Between Failure
MTTR	Meantime To Restoration
PFD	Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour The term “Probability” is misleading, as IEC 61508 defines a Rate.
PLC	Programmable Logic Controller
SFF	Safe Failure Fraction; summarises the fraction of -failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action. $SFF = (\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_D)$ $\lambda_S = \lambda_{SD} + \lambda_{SU}$ $\lambda_D = \lambda_{DD} + \lambda_{DU}$
SIL	Safety Integrity Level
SIS	Safety Instrumented System
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof test interval

Dräger Safety AG & Co. KGaA
Revalstraße 1
23560 Lübeck, Germany
Tel +49 451 882 0
Fax +49 451 882 20 80
www.draeger.com

90 33 034 - TM 4677.319

Edition 04 - July 2014 (Edition 01 - October 2007)
Subject to alteration