Knick

English

P 32*00P0/1

SIL Safety Manual

PolyTrans® P32000P0/1*

ThermoTrans® P32100P0/1*

SensoTrans® P32200P0/1*

SensoTrans® P32300P0/1*

www.knick.de

Table of Contents

1 Scope and Standards

This safety manual applies to the transmitters of the PolyTrans® P32000P0/1∗, ThermoTrans® P32100P0/1∗, SensoTrans® P32200P0/1∗, and SensoTrans® P32300P0/1∗ series.

Valid hardware and software versions:

- Serial number 1657362 or higher
- Device software Rev. 1.28 / 2.0 or higher

The safety-oriented series P32xxxP0/1∗ transmitters of Knick Elektronische Messgeräte GmbH & Co. KG are TÜV-certified to EN 61508 for use in SIL 2 applications (SIL 3 in a redundant configuration):

TÜV Rheinland Industrie Service GmbH
Automation, Software and Informations Technology (ASI)
Am Grauen Stein
D - 51105 Köln

Functional Safety
Type Approved
TÜVRheinland® FS

Certificate and Test Report No.: 968/EZ 272.00/07

The transmitters have been designed and tested in accordance with the following standards:

- **EN 61508: 2001**
  Functional safety of electrical/electronic/programmable electronic safety-related systems
- **EN 61511: 2004**
  Functional Safety – Safety instrumented systems for the process industry sector
- **EN 61010-1: 2001**
  Safety requirements for electrical equipment for measurement, control and laboratory use
- **EN 61326-1: 2006**
  Electrical equipment for measurement, control and laboratory use – EMC requirements
- **EN 61326-2-3: 2006**
  Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 2-3: Particular requirements – Test configuration, operational conditions and performance criteria for transducers with integrated or remote signal conditioning
- **IEC 61326-3-2: 2006**
  Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified EM environment
- **EN 50178: 1997**
  Electronic equipment for use in electric power plants

1.1 Abbreviations

Abbreviation	Description
SIL	Safety integrity level: Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest
PFD	Probability of dangerous failure on demand: Safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system
PFD_G	Average probability of failure on demand for the group of voted channels
PFH	Average frequency of a dangerous failure per hour: Average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time
PFH_G	Average frequency of dangerous failure for the group of voted channels
SFF	Safe failure fraction: Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures
λ	Total failure rate (per hour) of a channel in a subsystem
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0,5 λ (assumes 50 % dangerous failures and 50 % safe failures)
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)
λ_{SD}	Detected safe failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected safe failure rates within the channel of the subsystem)
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)
β	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)
HFT	Hardware fault tolerance: Capability of a functional unit to continue the execution of the demanded function in case of faults or deviations

Abbreviation	Description
MTBF	Mean time between failures
MTTR	Mean time to restoration (hour)
MRT	Mean repair time (hour)
FIT	Failure in time: 1×10^{-9} failures per hour
T_1	Proof test interval (hour)
T_2	Interval between demands (hour)
MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)
MooND	M out of N channel architecture with Diagnostics
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)

2 Device Description and Applications

2.1 Safety Function

The transmitters transfer the input signal with galvanic isolation and convert it into a standardized analog output signal of 0/4 - 20 mA or 0 - 5/10 V. The transfer function can be adapted to the sensors connected to the input. The analog output signal is routed to a logical unit (e.g. a PLC).

A one-channel architecture (1oo1) allows the use of devices up to SIL 2. A multi-channel, redundant architecture allows applications up to SIL 3. Here, the output signals of the transmitters are to be monitored by a suitable superordinated system (e.g. monitoring function in a PLC) which is safety oriented as 1oo2 system as defined in EN 61508 (see EN 61508-6, B 2.2.2).

2.2 Definition of Safe State

Output signal type	Safe state
0 – 20 mA	≤ 3.6 mA ; ≥ 21 mA
4 – 20 mA	≤ 3.6 mA ; ≥ 21 mA
0 – 10 V	≤ 0.1 V ; ≥ 10.5 V
0 – 5 V	≤ 0.1 V ; ≥ 5.25 V

3 Project Planning

3.1 Low Demand Mode

The transmitters are operated in low demand mode when the frequency of demands for operation made on the transmitters is no greater than one per year and no greater than twice the proof test frequency (EN 61508-4, 3.5.12).

The low demand mode can also be applied when the ratio of the internal diagnostic test rate of the transmitter to the demand rate exceeds the value 100 (EN 61508-2, 7.4.3.2.5).

An associated characteristic is the PFD value. It depends on the proof test interval T_1 between the functional tests of the safety function.

3.2 High Demand Mode

If the conditions for "low demand mode" do not apply, the transmitter must be applied as safety-related partial system in high demand or continuous mode (EN 61508-4, 3.5.12).

The fault tolerance time of the complete system must be higher than the sum of the reaction times or the diagnostic test intervals of all components in the safety-related measurement chain. An associated characteristic is the PFH value.

3.3 Types of Failures

A safe failure does not have the potential to set the safety-related system to a dangerous or impermissible state. The transmitter switches to the defined safe state or the fault mode, e.g. 21 mA when the measurement range is exceeded.

A dangerous undetected failure has the potential to set the safety-related system to a dangerous or impermissible state. The transmitter switches neither to the defined safe state nor to the fault mode.

3.4 Diagnostic Test Interval

In addition to safety functions, the transmitters continually perform diagnostic functions to detect faulty performance. The diagnostic test interval is the time during which these tests are completed and repeated. Accidental hardware faults are recognized within this time interval.

4 Assembly and Installation

The following documentation must be available for the respective transmitter:

PolyTrans® P32000P0/1x	ThermoTrans® P32100P0/1x	SensoTrans® P32200P0/1x	SensoTrans® P32300P0/1x
Operating instructions TA-254.111-KNExx	Operating instructions TA-254.113-KNExx	Operating instructions TA-254.114-KNExx	Operating instructions TA-254.115-KNExx

The notes, conditions, and limit values specified in the operating instructions must be observed during installation and operation of the transmitters.

For devices where a higher degree of availability is expected, overvoltage category III applies. The maximum working voltage for overvoltage category III and pollution degree 2 is 150 V AC/DC. For working voltages > 150 V AC/DC, suitable overvoltage protection measures shall be taken to ensure that overvoltage category III is achieved.

The wiring from the sensor at the point of measurement to the transmitter must be routed in a manner that prevents shorting between the conductors or with the surroundings.

When current (e.g. 4 … 20 mA) is configured as output signal, the output load must be ≥ 50 Ω.

Prior to commissioning and after each change of the configuration, the intended function of the transmitter must be checked (see section 5.1 “Functional Checks“).

If the configuration has been made using the IrDA® interface, the transmitter must then be set to Read-Only Mode. In this mode data can only be sent from the transmitter via the IrDA® interface (measured-value display, statistics, ...).

Activating the Read-Only Mode:

- All DIP switches = 0
- All rotary switches = 0

After completion of configuration the switches must be covered with the included self-adhesive polyimide tape.

5 Proof Tests

The proof test allows revealing dangerous faults which cannot be detected through self-diagnostics. Therefore, the correct functioning of the transmitters must be checked at appropriate intervals.

It is the responsibility of the operating company to choose the type of testing and the test intervals. The test intervals are, among others, determined when calculating the individual safety loops of a plant (PFD values).

The test must be carried out in a manner that verifies the flawless operation of the safety functions in conjunction with all components.

5.1 Functional Checks

The PFD values documented in section 6.x apply to the proof test interval T_1 = 1 year. The transmitter's operativeness must be checked in the application. Proceed as follows:

- Switch on the transmitter with open output (burden/load = ∞). Check the status and diagnostics messages indicated by LED:
  - Make sure that no device error (error message 10) is signaled.
  - When current (e.g. 4 … 20 mA) is configured as output signal, error message 6 (load output error) must be signaled.
- Adjust values for start and end of range and an average value (e.g. 50 % value). Check whether the measurement error lies within the specified tolerances.
- Verify the transition to the safe state. This test is preferably carried out by simulating an open circuit (open input). The output consequently shifts to ≥ 21 mA (current outputs) or ≥ 5.25 V or ≥ 10.5 V (voltage outputs). The “Sensor open“ error message is created (red LED blinks 4 times).

- The error signal is maintained after termination of the error cause (self-locking error message). The error message is reset by restart (power supply on/off or via IrDA).

If the functional test proves negative, the transmitter must be taken out of service and the process held in a safe state by means of other measures.

The transmitter itself is maintenance-free.

6 Safety-Related Characteristics

6.1 Assumptions

- Communication via IrDA interface is only used for configuring, adjusting, or diagnosing the device, but not for safety-relevant critical operations.
- After configuration (via rotary/DIP switches or IrDA interface) a functional test is performed to ensure that the measurement will be carried out conforming to the specifications.
- The mean repair time (MRT) after a device failure is max. 72 hours.
- The long-time average temperature is max. 55 °C.
- Ambient conditions correspond to an average industrial environment.
- The specifications of the operating instructions must be met.

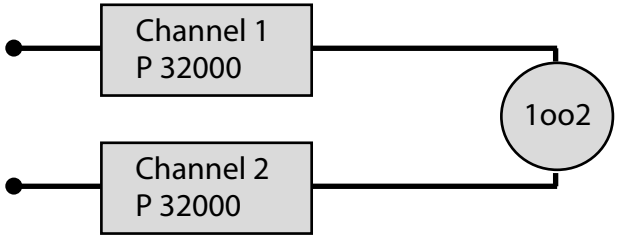
6.2 Specific Safety-Related Characteristics

Structure	1-channel (1oo1)
Category	SIL 2 (software: SIL 3)
Device type	Type B
HFT	0
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
PFD_{SIL2}	$2.7 \cdot 10^{-4}$
PFH_{SIL2}	$4.8 \cdot 10^{-8}$/h
PFD_{SIL3}	$4.9 \cdot 10^{-6}$
PFH_{SIL3}	$8.5 \cdot 10^{-9}$/h
Diagnostic test interval	< 5 s
Fault reaction time for overrange conditions	< 2 s
Failure rates:	
λ_S	759.2 FIT
λ_D	759.2 FIT
λ_{DU}	48.1 FIT
λ_{DD}	711.1 FIT

Note:
After 8 to 12 years, the failure rates of the electronic components will increase, whereby the derived PFD and PFH values will deteriorate (EN 61508-2, 7.4.7.4, note 3).

6.3 Sample Calculation

A typical double-redundant (1oo2) system with two PolyTrans P32000 transmitters is used as an example. The calculation has been performed in accordance with EN 61508: 2001 using PTC® Mathcad®.
The proof test interval T_1 is 1 year (8760 h).
To ensure correct operation of the safety function, the channels must be interconnected in such a manner that one channel is sufficient to trigger the safety function. Therefore, in a 1oo2 system a dangerous failure of the safety function occurs when both channels fail simultaneously.



$MTTR := 72\ hr$[1)] $\quad MRT := 72\ hr \quad FIT := \frac{1}{10^9\ hr} \quad \beta := 0.02 \quad \beta_D := 0.01$

$T_1 := 1 \cdot 8760\ hr$

$\lambda_{DU} := 48.1 \cdot FIT \quad \lambda_{DD} := 711.1 \cdot FIT \quad \lambda_D := 759.2 \cdot FIT \quad \lambda_S := 759.2 \cdot FIT$

$\frac{\lambda_{DU}}{\lambda_D} = 0.063 \quad \frac{\lambda_{DD}}{\lambda_D} = 0.937$

$$t_{CE} := \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_1}{2} + MRT \right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR = [349.5]\ hr$$

$$t_{GE} := \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_1}{3} + MRT \right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR = [257]\ hr$$

$$PFD := 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MRT \right)$$

$PFD = 4.896 \cdot 10^{-6}$

$$PFH := 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 \cdot t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} = [8.467 \cdot 10^{-9}] \frac{1}{hr}$$

[1)] Mathcad® uses hr as unit for hours.

The following values are obtained for this system:

Structure	2-channel (1oo2)
Category	SIL 3
Architecture	Type B
HFT	1
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
MRT	72 h
t_{CE}	349.5 h
t_{GE}	67.5 h
$PFD_{G,1oo2}$	$4.9 \cdot 10^{-6}$
$PFH_{G,1oo2}$	$8.5 \cdot 10^{-9}$/h

TÜVRheinland®
Genau. Richtig.

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 272.00/07

Prüfgegenstand **Product tested**	Messumformer-Reihe P32000	**Zertifikatsinhaber** **Holder of the certificate**	Knick Elektronische Messgeräte GmbH & Co. KG Beuckestrasse 22 14163 Berlin
Typbezeichnung **Type designation**	PolyTrans® P 32000 P0/1* SensoTrans® R P 32300 P0/1* SensoTrans® DMS P 32200 P0/1* ThermoTrans® P 32100 P0/1*	**Verwendungs-zweck** **Intended application**	Einsatz als Teil von Schutzein-richtungen zur Überwachung sicherheitsrelevanter Signale (Temperatur, Widerstand, Potentiometer, Spannung, ...)
Prüfgrundlagen **Codes and standards forming the basis of testing**	EN 61508:2001 EN 61511:2004 EN 61010-1:2001 EN 61326-1:2006 IEC 61326-3-2:2006 EN 50178:1997		
Prüfungsergebnis **Test results**	Die Messumformer-Reihe P32000 mit den oben genannten Typen erfüllt die gestellten Anforderungen der EN 61508 für SIL 2 bzw. SIL 3 im redundanten Betrieb und können in Schutzeinrichtungen zur Überwachung von sicherheitsrelevanten Prozessgrössen ein-gesetzt werden.		
Besondere Bedingungen **Specific requirements**	Die Sicherheitshinweise im Sicherheitshandbuch und in den Gebrauchsanleitungen der Messumformer sind zu berück-sichtigen.		

Functional Safety
Type Approved
TÜVRheinland® FS

Der Prüfbericht-Nr.: 968/EZ 272.00/07 vom 12.10.2007 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no.: 968/EZ 272.00/07 dated 12.10.2007 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

12.10.2007
Datum/Date

Firmenstempel/Company Seal

Dipl.-Ing. Klaus Kemp

Knick
Elektronische Messgeräte
GmbH & Co. KG

Beuckestr. 22 • 14163 Berlin
Germany

Phone: +49 30 80191-0
Fax: +49 30 80191-200
info@knick.de
www.knick-international.com

Version: 1.1
This manual was last updated on April 10, 2018

The latest documents are available for download on our website under the corresponding product description.

094229

20180410
TS-254.111-KNE02