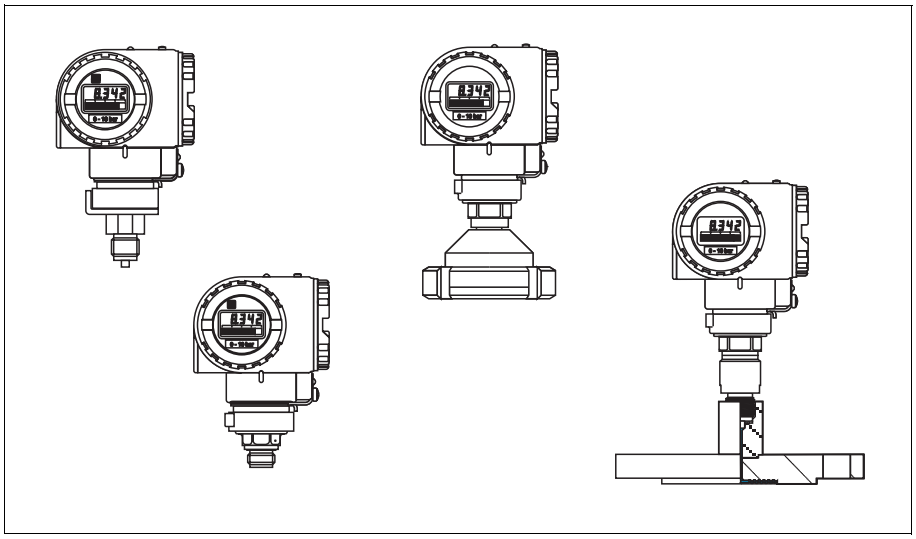
Safety Manual
SD 159P/00/en

# Pressure Transmitter
# *cerabar S PMC 731/631*
# *cerabar S PMP 731/635*
# *with 4...20 mA output signal*

## Functional safety manual



**Application**
Pressure measurements (e.g. limit pressure monitoring) to satisfy particular safety systems requirements as per IEC 61508/ IEC 61511-1 (FDIS).

The measuring device fulfils the requirements concerning
- Functional safety as per IEC 61508/IEC 61511-1 (FDIS)
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per EN 61326 and NAMUR recommendation NE 21.

**Your benefits**
- Used for limit pressure monitoring up to SIL 2, independently evaluated (Functional Assessment) by TÜV Rheinland as per IEC 61508/ IEC 61511-1 (FDIS)
- Continuous measurement
- Easy commissioning

Endress+Hauser
The Power of Know How

# Table of contents

# SIL declaration of conformity

SIL-03003a/00/e

**ENDRESS + HAUSER**

## SIL Declaration of Conformity

**Functional safety of a smart differential pressure transmitter according to IEC 61508/IEC 61511-1 (FDIS)**

**Endress+Hauser GmbH+Co. KG, Hauptstrasse 1, 79689 Maulburg**

declares as manufacturer, that the differential pressure transmitter

**Cerabar S PMP731/635, PMC731/635/631 (4...20 mA)**

are suitable for the use in a safety instrumented system up to SIL 2 according to the standard IEC 61511-1 (FDIS), if the enclosed safety instructions are observed.

The analysis of safety critical and dangerous faults provides under the assumption of an annual functional test cycle the following parameters:

| | |
|---|---|
| SIL (Safety integrity level) | 2 |
| HFT (Hardware fault-tolerance) | 0[1] (single channel use) |

| | PMP731/635 | PMC731/635/631 |
|---|---|---|
| SFF (Safe failure fraction) | 88.1 % | 82.4 % |
| $PFD_{av}$ (Average probability of failure on demand)[2] | $4.14 \times 10^{-4}$ | $6.43 \times 10^{-4}$ |
| $MTBF_{tot}$ (Mean time between total failures) | 143 years | 137 years |
| $\lambda_{safe} + \lambda_{DD}$ (Sum of safe and dangerous detected failure rates) | 700.8 FIT | 685.7 FIT |
| $\lambda_{DU}$ (Dangerous undetected failure rate) | 94.4 FIT | 146.9 FIT |

[1] according to clause 11.4 of IEC 61511-1(FDIS)
[2] the PFDav values are also within the range for SIL2 according to ISA S84.01.

The assessment of the proven-in-use demonstration covers the device and its software including the modification process.

Maulburg, January 29, 2003

Endress+Hauser GmbH+Co. KG

i.V. Manager Certification i.V. Projectmanager

P01-PMxx3xxx-02-xx-xx-en-000

# Introduction

**Abbreviations, standards and terms**

## Abbreviations

| Abbreviation | Explanation |
|---|---|
| HFT | Hardware Fault Tolerance<br>*Ability of a functional unit (hardware) to continue to perform a required function in the presence of faults or errors.* |
| MTBF | Mean Time Between Failures |
| MTTR | Mean Time To Repair |
| PFD | Probability of Failure on Demand |
| $PVD_{av}$ | Average Probability of Failure on Demand |
| SIL | Safety Integrity Level<br>*The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for the failure of a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will not perform the requested safety function.* |
| SFF | Safe Failure Fraction<br>*Fraction of failures which do not have the potential to put the safety-related system in a hazardous or fail-to-function state.* |
| TI | Test interval between life testing of the safety function |
| XooY | "X out of Y" voting<br>*Classification and description of the safety-related system with regard to redundancy and selection procedure used.*<br>*"Y" specifies how often the safety function is performed (redundancy).*<br>*"X" determines how many channels have to work properly.*<br>*Pressure measurement example: 1oo2 architecture – A safety-related system decides that a predefined pressure limit is exceeded when one of two pressure sensor reaches this limit. If a 1oo1 architecture is used, there is only one pressure sensor available.* |

## Relevant standards

| Standard | Explanation |
|---|---|
| IEC 61508,<br>Part 1 – 7 | Functional safety of electrical/electronic/programmable electronic safety-related systems<br>(Target group: Manufacturers and Suppliers of Devices) |
| IEC 61511<br>Part 1 – 3 (FDIS) | Functional safety – Safety Instrumented Systems for the process industry sector<br>(Target group: Safety Instrumented Systems Designers, Integrators and Users) |

**Terms**

| Term | Explanation |
|---|---|
| Dangerous failure | Failure with the potential to put the safety-related system in a dangerous or non-functional condition. |
| Safety-related system | A safety-related system performs the safety functions that are required to achieve or maintain a safe condition e.g. in a plant. Example: pressure measuring device – logic unit (e.g. limit signal generator) – valve form a safety-related system. |
| Safety function | Defined function, which is performed by a safety-related system with the aim of achieving or maintaining a safe condition for the plant, considering a specified dangerous incident. Example: limit pressure monitoring |

## Determining the Safety Integrity Level (SIL)

The achievable Safety Integrity Level is determined by the following safety-related parameters:
- Average Probability of Failure on Demand ($PFD_{av}$)
- Hardware Fault Tolerance (HFT) and
- Safe Failure Fraction (SFF).

The specific safety-related parameters for the Cerabar S, as a part of a safety function, are listed in the "Safety-related parameters" chapter.

The following table displays the dependence of the "Safety Integrity Level" (SIL) on the "Average Probability of Failure on Demand" ($PFD_{av}$). Here, the "Low demand mode" has been observed, i.e. the requirement rate for the safety-related system is maximum once a year.

| Safety Integrity Level (SIL) | $PFD_{av}$ (Low demand mode) |
|---|---|
| 4 | $\geq 10^{-5} ... < 10^{-4}$ |
| 3 | $\geq 10^{-4} ... < 10^{-3}$ |
| 2 | $\geq 10^{-3} ... < 10^{-2}$ |
| 1 | $\geq 10^{-2} ... < 10^{-1}$ |

Sensor, logic unit and actuator together form a safety-related system, which performs a safety function. The "Average Probability of Failure on Demand" ($PFD_{av}$) is usually divided up into the sensor, logic unit and actuator sub-systems as per Figure 1.

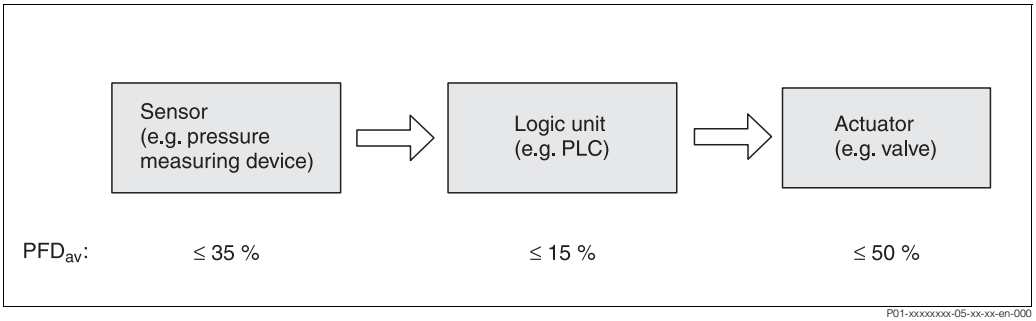



*Fig. 1: usual division of the "Average Probability of Failure on Demand" ($PFD_{av}$) into the sub-systems*

**Note!**
This documentation considers the Cerabar S as a component of a safety function.

The following table displays the achievable "Safety Integrity Level" (SIL) of the entire safety-related system for type B systems depending on the "Safe Failure Fraction" (SFF) and the "Hardware Fault Tolerance" (HFT). Type B systems are, for example, sensors with complex components such as microprocessors (→ see also IEC 61508, Part 2).

| **Safe Failure Fraction (SFF)** | **Hardware Fault Tolerance (HFT)** | | |
|---|---|---|---|
| | **0** | **1 (0) [1]** | **2 (1)** [1] |
| <60% | not permitted | SIL 1 | SIL 2 |
| 60 ...<90% | SIL 1 | **SIL 2** | SIL 3 |
| 90 ...<99% | SIL 2 | SIL 3 | – |
| ≥ 99 % | SIL 3 | – | – |

1) In accordance with IEC 61511-1 (FDIS), Clause 11.4.4, the "Hardware Fault Tolerance" (HFT) can be reduced by one (values in brackets), if the following conditions are true for devices using sensors and actuators with complex components:
– The device is "proven in use".
– The device allows adjustment of process-related parameters only, e.g. measuring range, upscale or downscale failure direction, etc.
– The adjustment level of the process-related parameters of the device is protected, e.g. by jumper, password (here: numeric code or key combination)
– The function has a "Safety Integrity Level" (SIL) requirement less than 4.
All conditions are true for the Cerabar S.

# Safety function with Cerabar S

**Safety function for limit pressure monitoring**

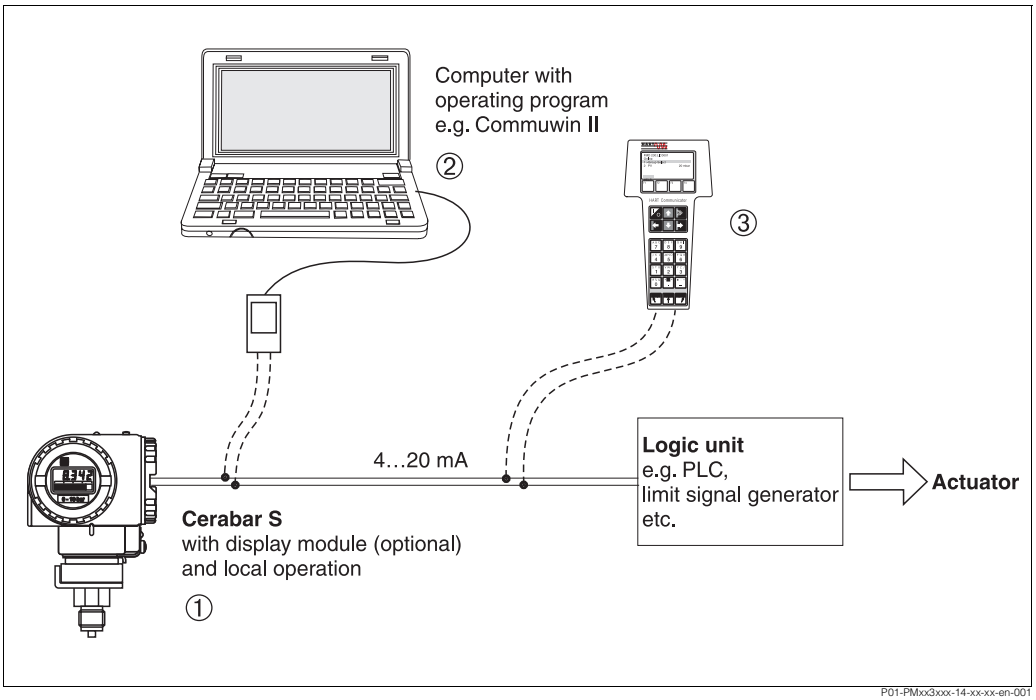



*Fig. 2: safety function (e.g. for limit pressure monitoring) with Cerabar S as sub-system*

*1 Cerabar S with local operation, option for setting the lower-range value and upper-range value and the attenuation*
*2 Computer with operating program e.g. Commuwin II for setting all parameters such as alarm behaviour, max. alarm, operating mode, etc.*
*3 Handheld terminal Hart Communicator DXR 275 for setting all parameters such as alarm behaviour, max. alarm, operating mode, etc.*

The Cerabar S transmitter generates an analogue signal (4...20 mA) proportional to the pressure. The analogue signal is fed to a downstream logic unit, such as a PLC or limit signal generator, and there it is monitored to determine whether it exceeds a maximum value. In order to monitor for faults, the logic unit must be able to detect both HI-alarms (adjustable from 21...22.5 mA) and LO-alarms (3.6 mA).

**Safety function data**

**Caution!**
The compulsory settings and data for the safety functions are listed in the "Settings" and "Safety-related parameters" chapters.

For the reaction time of the transmitter, see Technical Information TI 216P (PMC 731 and PMP 731) or Technical Information TI 217P (PMC 631 and PMP 635).

**Note!**
MTTR is set at eight hours.
Safety-related systems without a self-locking function must be monitored or set to an otherwise safe state after carrying out the safety function within MTTR.

**Supplementary device documentation**

Depending on the version, the following documentation must be available for the transmitter:

| Explosion protection/ Certificates | Devices | Operating Instructions (BA) | Other documentation (XA, ZE or ZD) |
|---|---|---|---|
| None | PMC 731, PMP 731, PMC 631, PMP 635 | BA 187P | none |
| ATEX II 1/2 G<br>EEx ia IIC T4/T6 | PMC 731, PMP 731, PMC 631, PMP 635 | BA 187P | Safety Instructions<br>XA 001P |
| ATEX II 3 G<br>EEx nA II T6 | PMC 731, PMP 731, PMC 631, PMP 635 | BA 187P | Safety Instructions<br>XA 150P |
| ATEX II 2 G<br>EEx d[ia] IIC T5/T6 | PMC 731, PMC 635 | BA 187P | Safety Instructions<br>XA 053P |
| ATEX II 2 G<br>EEx d IIC T5/T6 | PMP 731, PMP 635 | BA 187P | Safety Instructions<br>XA 022P |
| CSA IS (non incendive)<br>Class I, II, III; Div. 1, Groups A – G | PMC 731, PMP 731, PMC 631, PMP 635 | BA 187P | ZD 022P |
| CSA Explosion proof<br>Class I, II, III; Div. 1; Groups B – G | PMP 731, PMP 635 | BA 187P | none |
| FM IS (non-incendive)<br>Class I, II, III; Div. 1, Groups A – G | PMC 731, PMP 731, PMC 631, PMP 635 | BA 187P | 960338-1030 |
| FM Explosion proof<br>Class I, II, III, Div. 1; Groups A – G | PMP 731, PMP 635 | BA 187P | none |

**Caution!**
- The installation and setting instructions, and the technical limit values must be observed in accordance with the Operating Instructions (BA 187P).
- For devices which are used in explosion-hazardous, the supplementary documentation (XA, ZD) must also be used in accordance with the table.

**Cerabar S supplementary documentation**
For further information, see Technical Information TI 216P (PMC 731 and PMP 731) or Technical Information TI 217P (PMC 631 and PMP 635).

# Behaviour in operation and failure

**Note!**
The behaviour in operation and failure is described in the Operating Instructions BA 187P.

# Iterative tests

**Using the Cerabar S for continuous measurements**

The operability of the measuring device must be tested at appropriate time intervals. We recommend carrying out the test at least once a year. It is the responsibility of the user to select the type of check and the intervals in the specified time frame.

# Settings

**Alarm behaviour and current output**

In the event of a fault, the current value is set to the value you have selected. The settings can be made either using the Endress+Hauser Commuwin II operating program or with the HART Communicator DXR 275 handheld terminal. Use the "Set output safety" or "Alarm mode" parameters to set the alarm behaviour. Use the "Set max. current" or "Max. alarm current" parameters to set the maximum alarm current.

| **"Set output safety" or "Alarm behaviour" selection** | **Current value in the event of a fault** |
|---|---|
| "Min" or "Min. alarm" | 3.6 mA |
| "Max" or "Max. alarm" | Can be set via "Set max. current" or "Max. alarm current" parameters: 21...22.5 mA.<br>Factory setting: 22 mA |

| **Software version** | **Matrix position (only for operation via Commuwin II)** | **Parameter** | **Permitted settings** | **⚠ Caution! Impermissible setting!** |
|---|---|---|---|---|
| SW 7.0 | V0H8 | Set output safety | – Min (–10 %)<br>– Max (110 %) | Continue (this setting is not permitted for the safety function!) |
| | V9H4 | Set max. current | 21...22.5 mA | |
| SW 7.1 | V0H8 | Alarm mode | – Min. alarm<br>– Max. alarm | Value hold (this setting is not permitted for the safety function!) |
| | V9H4 | Max. alarm current | 21...22.5 mA | |

**Warning!**
**When using the device as a component of a safety function, the "Continue" or "Value hold" setting must not be selected!**

**Checks**

**Caution!**
After entering all of the parameters, check the safety function. The Cerabar S offers the option of simulating a signal current via the "Simulation" and "Set simulation current" parameters, independently of the measured pressure. (This parameters are available when using Commuwin II and the HART handheld terminal.) → See also the Operating Instructions BA 187P, chapter 7.2 "Current simulation".

**Locking/Unlocking**

**Warning!**
Changes to the measuring system and its settings after commissioning can have a negative effect on the safety function. For this reason, you should lock operation of the Cerabar S via the keys on the device after entering all parameters and checking the safety function. This protects your entries against undesired and unauthorised changes.

Security locking via the keys on the device can also only be unlocked again via the keys on the device.

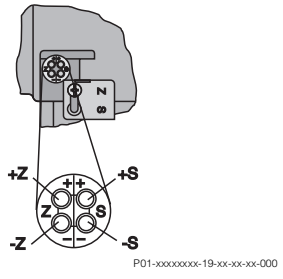



*Fig. 3: Keys on the device*


**Lock operation:**
Press +Z and –S once simultaneously.


**Unlock operation:**
Press +S and –Z once simultaneously.

**Caution!**
The locking and unlocking function is also available via the Commuwin II operating program and the Hart Communicator DXR 275. To ensure that unlocking via communication is ruled out, you should always lock operation via the keys on the device.

# Safety-related parameters

**Specific safety-related parameters for Cerabar S**

The table displays the specific safety-related parameters for the Cerabar S.

| | PMP 731 | PMP 635 | PMC 731 | PMC 631 |
|---|---|---|---|---|
| SIL | SIL 2 | | SIL 2 | |
| HFT | 0 | | 0 | |
| SFF | 88.1 % | | 82.4 % | |
| $PFD_{av}$ | $4.14 \times 10^{-4}$ | | $6.43 \times 10^{-4}$ | |
| TI [1] | annual | | annual | |

1) Complete function test, e.g. by approaching level

**$PFD_{av}$ dependent on selected maintenance interval**

The following diagram presents the dependence of the $PFD_{av}$ on the maintenance interval. The $PFD_{av}$ increases as the maintenance interval increases.

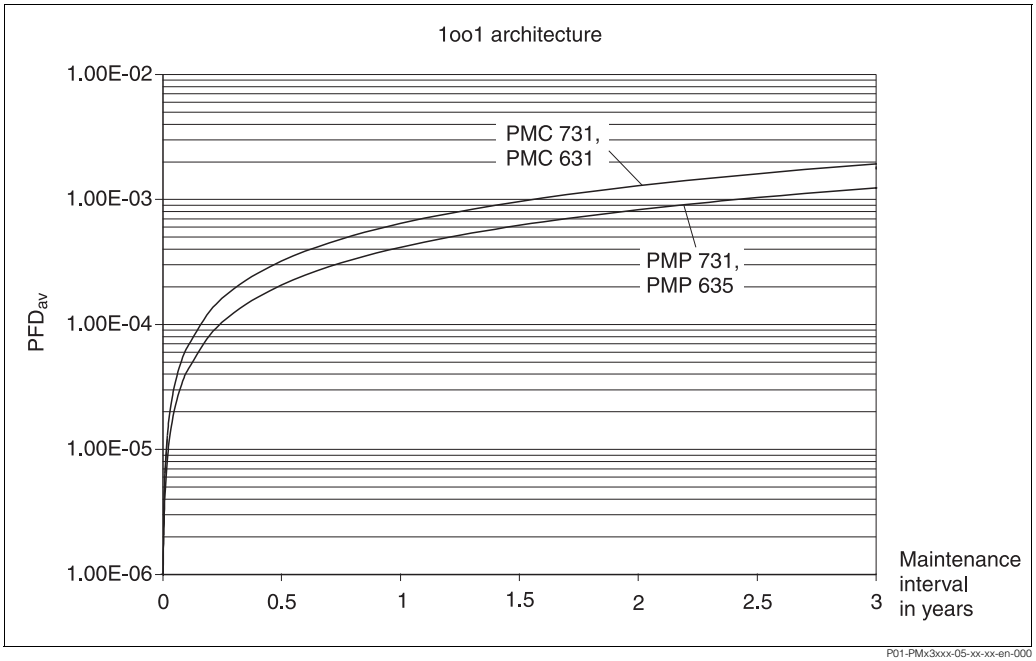



*Fig. 4: "Average Probability of Failure on Demand" ($PFD_{av}$) dependent on the selected maintenance interval*

# TÜV management summary

2003-01-27

TÜV Rheinland
Berlin Brandenburg

**Automation, Software and Information Technology**

**Test report about the determination of safety-related parameters according to IEC 61508 and IEC 61511 (FDIS) for the Endress+Hauser smart pressure transmitters Cerabar S, smart differential pressure transmitters Deltabar S and pressure transducers Cerabar T**

**Report-No.: 968/EL 193.00/03**
**Date: 2003-01-27**



2003-01-27

TÜV Rheinland
Berlin Brandenburg

## 5. Summary

Based on the submitted manufacturer documents an assessment of safety relevant parameters (failure rates, $PFD_{av,}$ HFT and SFF) has been carried out for different pressure sensors, manufactured by the Endress+Hauser company. The assessment, that covers the pressure instruments type Cerabar S, Deltabar S and Cerabar T, was carried out in compliance with the requirements of IEC 61508 and IEC 61511 (FDIS).

The assessment showed the following results:

**Type A component: Cerabar T PMP131**

The safety relevant parameters $PFD_{av,}$ HFT and SFF are in compliance with the corresponding requirements for **SIL 2** according to IEC 61508.

**Type B components: Cerabar S, Deltabar S, Cerabar T PMC131**

The safety relevant parameter $PFD_{av}$ is in compliance with the corresponding requirements for **SIL 2** according to IEC 61508.

The safety relevant parameters HFT and SFF are in compliance with the corresponding requirements for **SIL 1** according to IEC 61508.

The safety relevant parameters HFT and SFF are in compliance with the corresponding requirements for **SIL 2** according to IEC 61511(FDIS).

The user should consider, that the hardware fault tolerance of all inspected devices is zero and that a single fault can lead to a dangerous failure.

**NOTES:**

The assessment results described in this report only refer to the safety-related parameters $PFD_{av}$, HFT and SFF according to IEC 61508 and IEC 61511 (FDIS).

This report does not make any statements, that the manufacturer meets all other requirements of the above cited standards for hardware, software, documentation, management of functional safety, verification and validation.

This report does not imply that the examined pressure sensors have been certified for functional safety by the assessor according to IEC 61508 or any other standards.

The pressure sensors are only one part of a complete safety function. It is at the responsibility of the end-user to prepare and to apply an extensive reliability model, that brings out the complete safety function and that meets all requirements of the claimed SIL level according to IEC 61508.

Cologne, 2003-01-27
ASI/Kst. 968 ja-nie

The inspector



Dipl.-Phys. Erich Janoschek

**Endress+Hauser GmbH+Co.**
Instruments International
P.O. Box 2222
D-79574 Weil am Rhein
Germany

Tel. (07621) 975-02
Tx 773926
Fax (07621) 975 345
e-mail: info@ii.endress.com

**Internet:**
http://www.endress.com

Endress + Hauser
The Power of Know How

11.01

SD 159P/00/en/01.03a
FM+SGML 6.0 ProMoDo