FY01025P/00/EN/04.24-00
71671715
2024-08-01

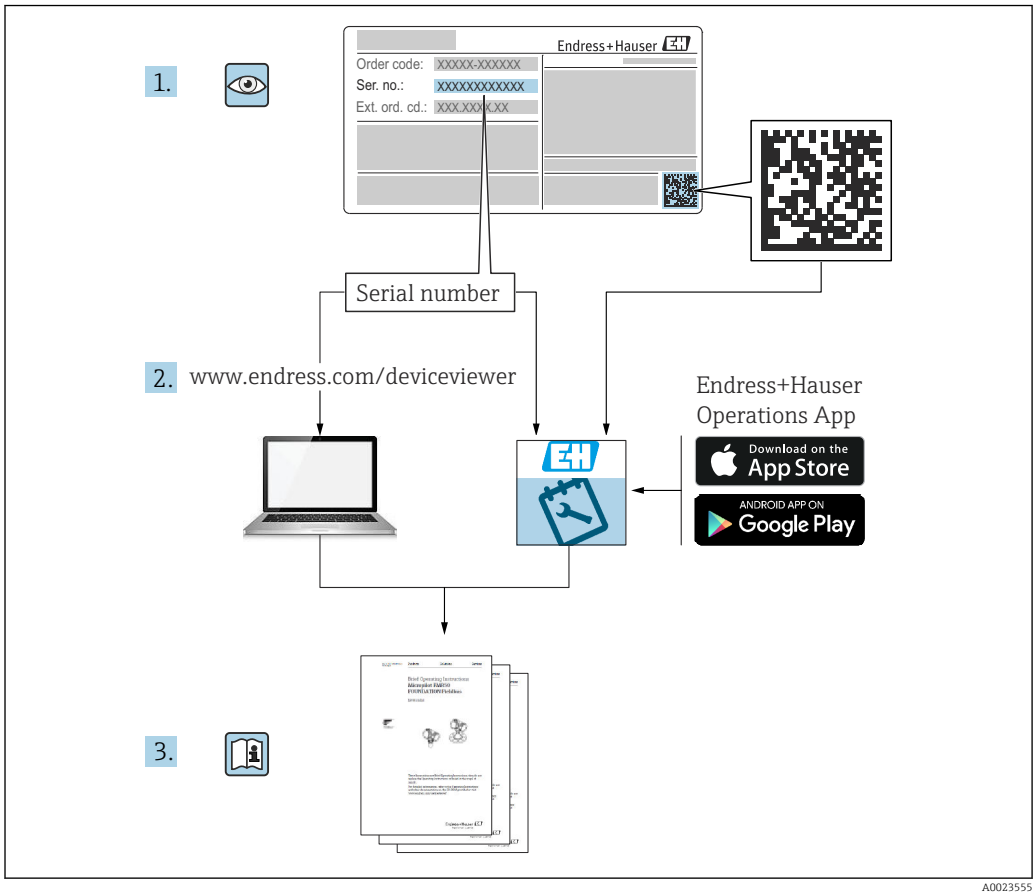
01.01.zz (Device firmware)



# Functional Safety Manual
# **Cerabar PMC51B**

Process pressure measurement
Pressure transmitter with ceramic measuring cell

Endress+Hauser
People for Process Automation


1.
Endress+Hauser
Order code: XXXXX-XXXXXX
Ser. no.: XXXXXXXXXXX
Ext. ord. cd.: XXX XXX XX
Serial number
2. www.endress.com/deviceviewer
Endress+Hauser
Operations App
Download on the App Store
ANDROID APP ON Google Play
3.
A0023555

# Table of contents

# 1 Declaration of Conformity

SIL_00419_04.24

Endress+Hauser
People for Process Automation

## Declaration of Conformity

Functional Safety according to IEC 61508
Based on NE 130 Form B.1

Endress+Hauser SE+Co. KG, Hauptstraße 1, 79689 Maulburg

being the manufacturer, declares that the product

Cerabar PMC51B

is suitable for the use in safety-instrumented systems according to IEC 61508. The instructions of the corresponding functional safety manual must be followed.

This declaration of conformity is exclusively valid for the listed products and accessories in delivery status.

Maulburg, April 2, 2024
Endress+Hauser SE+Co. KG

i. V. E-SIGNED by Gerd Bechtel
on 07 April 2024 21:09:50 CEST

Gerd Bechtel
Dept. Man. R&D Devices Pressure
Research & Development

i. V. E-SIGNED by Manfred Hammer
on 03 April 2024 08:17:15 CEST

Manfred Hammer
Dept. Man. R&D Quality Management/FSM
Research & Development

A0043073

# 1.1 Safety-related characteristic values

SIL_00419_04.24

Endress+Hauser
People for Process Automation

| | | | |
|---|---|---|---|
| **General** | | | |
| Device designation and permissible types [1] | Cerabar PMC51B ** BA * * * * ** * ** *** * + [LA ] | | |
| | | | |
| Safety-related output signal | 4... 20 mA | | |
| Fault signal | ≤ 3.6 mA / ≥ 21.0 mA | | |
| Process variable/function | Pressure and level measurement | | |
| Safety function(s) | MIN / MAX / RANGE | | |
| Device type acc. to IEC 61508-2 | ☐ Type A | ☒ Type B | |
| Operating mode | ☒ Low Demand Mode | ☒ High Demand Mode | |
| Valid hardware version | 01.00.ww (ww: any double number) | | |
| Valid software version | 01.01.zz (zz: any double number) | | |
| Safety manual | FY01025P | | |
| Type of evaluation (check only one box) | ☒ | Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3 | |
| | ☐ | Evaluation of "proven in use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3 | |
| | ☐ | Evaluation of HW/SW field data to verify „prior use" acc. to IEC 61511 | |
| | ☐ | Evaluation by FMEDA acc. to IEC 61508-2 for devices w/o software | |
| Evaluation through – report/certificate no. | TÜV Süd Z10 020351 0009 | | |
| Test documents | Development documents | Test reports | Data sheets |
| **SIL – Integrity** | | | |
| Systematic safety integrity | | ☐ SC 2 | ☒ SC 3 |
| Hardware safety integrity | Single channel use (HFT = 0) | ☒ SIL 2 capable | ☐ SIL 3 capable |
| | Multi channel use (HFT ≥ 1) | ☐ SIL 2 capable | ☒ SIL 3 capable |

| **FMEDA** | | | |
|---|---|---|---|
| Safety function | MIN | MAX | RANGE |
| $\lambda_{DU}$ [2),3)] | 25 FIT | 25 FIT | 25 FIT |
| $\lambda_{DD}$ [2),3)] | 1233 FIT | 1233 FIT | 1233 FIT |
| $\lambda_S$ [2),3)] | 573 FIT | 573 FIT | 573 FIT |
| SFF | 99% | 99% | 99% |
| $PFD_{avg}$ ($T_1$ = 1 year)[3)] (single channel architecture) | $1.1 \cdot 10^{-4}$ | $1.1 \cdot 10^{-4}$ | $1.1 \cdot 10^{-4}$ |
| PFH | $2.5 \cdot 10^{-8}$ 1/h | $2.5 \cdot 10^{-8}$ 1/h | $2.5 \cdot 10^{-8}$ 1/h |
| PTC [4)] A / B | 95% / 61% | 95% / 61% | 95% / 61% |
| Diagnostic test interval [5)] | ≤ 30 min | ≤ 30 min | ≤ 30 min |
| Fault reaction time [6)] | ≤ 5 s | ≤ 5 s | ≤ 5 s |

| **Comments** |
|---|
| – |

| **Declaration** | |
|---|---|
| ☒ | Our internal company quality management system ensures information on safety-related systematic faults which become evident in the future |

[1)] Valid order codes and order code exclusions are maintained in the E+H ordering system
[2)] FIT = Failure In Time, number of failures per $10^9$ h
[3)] Valid for average ambient temperature up to +40 °C (+104 °F)
For continuous operation at ambient temperature close to +60 °C (+140 °F), a factor of 2.1 should be applied
[4)] PTC = Proof Test Coverage
[5)] All diagnostic functions are performed at least once within the diagnostic test interval
[6)] Maximum time between error recognition and error response

A0043074

# 2 About this document

## 2.1 Document function

This supplementary Safety Manual applies in addition to the Operating Instructions, Technical Information and ATEX Safety Instructions. The supplementary device documentation must be observed during installation, commissioning and operation. The requirements specific for the protection function are described in this Safety Manual.

General information on functional safety (SIL) is available at:
- www.endress.com/SIL
- WP01032F, Whitepaper "Functional Safety in practice"

## 2.2 Symbols used

### 2.2.1 Safety symbols

DANGER
This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.

WARNING
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.

CAUTION
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.

NOTICE
This symbol contains information on procedures and other facts which do not result in personal injury.

### 2.2.2 Symbols for certain types of information and graphics

**Tip**
Indicates additional information

Reference to documentation

Reference to graphic

▶
Notice or individual step to be observed

1., 2., 3.
Series of steps

Result of a step

**1, 2, 3, ...**
Item numbers

**A, B, C, ...**
Views

## 2.3 Supplementary device documentation

For an overview of the scope of the associated Technical Documentation, refer to the following:
- *Device Viewer* (www.endress.com/deviceviewer): Enter the serial number from the nameplate
- *Endress+Hauser Operations app*: Enter serial number from nameplate or scan matrix code on nameplate.

The following document types are available in the download area of the Endress+Hauser website (www.endress.com/downloads):

### 2.3.1 Further applicable documents

- TI01506P
- BA02009P
- KA01469P
- GP01165P

### 2.3.2 Technical Information (TI)

**Planning aid**
The document contains all the technical data on the device and provides an overview of the accessories and other products that can be ordered for the device.

### 2.3.3 Operating Instructions (BA)

**Your reference guide**
These Operating Instructions contain all the information that is required in various phases of the life cycle of the device: from product identification, incoming acceptance and storage, to mounting, connection, operation and commissioning through to troubleshooting, maintenance and disposal.

### 2.3.4 Brief Operating Instructions (KA)

**Guide that takes you quickly to the 1st measured value**
The Brief Operating Instructions contain all the essential information from incoming acceptance to initial commissioning.

### 2.3.5 Description of Device Parameters (GP)

**Parameter reference document**
The document is part of the Operating Instructions and provides a detailed explanation of each individual parameter in the operating menu.

### 2.3.6 Certificate

The associated certificate is available in the Endress+Hauser Device Viewer (Section 2.3) or can be found in the Declaration of Conformity (Section 1) of the applicable Functional Safety Manual. This certificate must be valid at the time of delivery of the device.

# 3 Design

## 3.1 Permitted devices types

The details pertaining to functional safety in this manual relate to the device versions listed below and are valid as of the specified firmware and hardware versions.

Unless otherwise specified, all subsequent versions can also be used for safety functions.

A modification process according to IEC 61508:2010 is applied for any device modifications.

Any exemptions from possible combinations of features are saved in the Endress +Hauser ordering system.

Valid device versions for safety-related use:

### 3.1.1 Order codes

**PMC51B-**

**Feature: 010 "Approval"**
Version: all

**Feature: 020 "Output"**
Version: BA ; 2-wire 4-20mA HART

**Feature: 030 "Display, operation"**
Version: all

**Feature: 040 "Housing; material"**
Version: all

**Feature: 050 "Electrical connection"**
Version: all

**Feature: 055 "Pressure type"**
Version: all

**Feature: 075 "Sensor range"**
Version: all

**Feature: 090 "Calibration; unit"**
Version: all

**Feature: 105 "Process connection, sealing surface"**
Version: all

**Feature: 110 "Process connection"**
Version: all

**Feature: 200 "Seal"**
Version: all

**Optional:**

**Feature: 545 "Reference accuracy"**
Version: all

**Feature: 550 "Calibration"**
Version: all

**Feature: 570 "Service"**
Version: all

**Feature: 580 "Test, certificate, declaration"**
Version: all

**Feature: 590 "Additional approval"**
Version: all
The version **"LA"** must be selected for use as a safety function as per IEC 61508.

**Feature: 600 "Sensor design"**
Version: all

**Feature: 610 "Accessory mounted"**
Version: all

**Feature: 620 "Accessory enclosed"**
Version: all

**Feature: 660 "Regional device adaptation"**
Version: all

**Feature: 850 "Firmware version"**
Version: all

**Feature: 895 "Marking"**
Version: all

## 3.2 Identification marking

SIL-certified devices are marked with the SIL logo on the nameplate.

## 3.3 Safety function

The device's safety functions are:
- Minimum, maximum or range monitoring
- Absolute pressure measurement
- Gauge pressure measurement

For the safety function, the limit values for maximum or minimum monitoring must be defined by the user at a downstream logic unit (e.g. PLC, level switch etc.) for the safety-related output signal.

The same safety-related characteristic values that apply for range monitoring also apply for maximum or minimum monitoring.

Internal device errors result in a failure current at the analog output if safe measuring operation is no longer possible.

The assessment of the functional safety of a device includes the basic unit with the main electronics, sensor electronics and sensor up to the sensor membrane and the process connection mounted directly on the device. Process adapters and mounted/ enclosed accessories are not taken into account in the rating.

Detailed measurement errors, such as for other temperature ranges, can be calculated with the "Sizing Pressure Performance" Applicator.

A0038927

*1 QR code for the "Sizing Pressure Performance" Applicator*

Responsibility for assessing the suitability of the entire system - consisting of the basic unit and accessories - for safety-related use lies with the operator.

- Pay attention to the planning information provided in the usual standards
- Pay attention to the Technical Information ("Supplementary device documentation")

### 3.3.1 Safety-related output signal

The device's safety-related signal is the analog output signal 4 to 20 mA. All safety measures refer to this signal exclusively. The device additionally communicates for information only via HART and contains all HART features with additional device information. HART communication is not part of the safety function. The behavior of the output current in the event of an error depends on the setting for the messages. The safety-related output signal is fed to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter where it is monitored for the following:

- To ascertain if it exceeds or drops below a predefined limit value
- The occurrence of a fault, e.g. error current (≤ 3.6 mA, ≥ 21.0 mA, interruption or short-circuit of the signal line).

NOTICE

**In an alarm condition**

▶ Ensure that the equipment under control achieves or maintains a safe state.

The following dangerous undetected failures can occur in the devices:
- An incorrect output signal that deviates from the real value by more than 2%, wherein the output signal is still in the range of 4 to 20 mA or 3.8 to 20.5 mA.
- A settling time that is delayed by more than the specified settling time plus tolerance.

For failure monitoring, the logic unit must recognize both HI alarms (≥ 21.0 mA) and LO alarms (≤ 3.6 mA).

The transmitter output is not safety-oriented in the following situations:
- Configuration changes
- Proof testing
- Simulation

### 3.3.2 Safe measurement

The transmitter's safety function comprises a transmitted current output signal that is proportional to the pressure value. All safety functions can be used in combination with all sensor configurations from the "Structure of the measuring system" section.

### 3.3.3 Redundant configuration of multiple sensors

This section provides additional information regarding the use of homogeneously redundant sensors e.g. in a 1oo2 or 2oo3 architecture. The failure rates for HFT = 1 are based on an analysis in accordance with:

DIN EN 61508-6: 2011-02, Table D.4, "Using the β-factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures."

The device meets the requirements for SIL 3 in homogeneously redundant applications. The following common cause factors β and βD can be used for the design.

- β for homogeneously redundant use: 5 %
- βD for homogeneously redundant use: 2%

The system-specific analysis can produce other values depending on the specific installation and use of additional components.

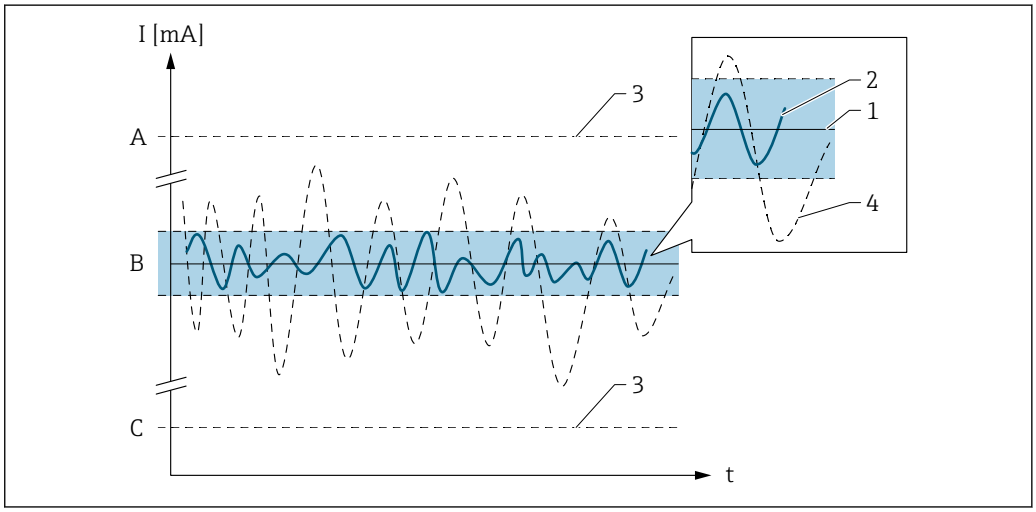
The following are possible measures to reduce the common cause factors:
- Sensors installed in a physically separate location
- Cables routed separately
- Separate protection from environmental influences, e.g.:
  - Impact
  - Sunshine
  - EMC and/or overvoltage

## 3.4 Basic conditions for use in safety-related applications

The device must be used correctly for the specific application, taking into account the medium properties and ambient conditions. Carefully follow instructions pertaining to critical process situations and installation conditions from the Operating Instructions. The application-specific limits must be observed. The specifications in the Operating Instructions and the Technical Information must not be exceeded.

The stability particularly of the wetted materials must be guaranteed and must be verified by the user.

### 3.4.1 Random failures in accordance with IEC/EN 61508




*A HI alarm ≥ 21 mA*
*B SIL error range ±2%*
*C LO alarm ≤ 3.6 mA*

**No device error**
- No failure
- No impact on the safety-related output signal
- Implications for the safety-related output signal:
  1 – Within the specification (TI, BA etc.)

**$\lambda_S$ (Safe)**
- Safe failure
- No impact on the safety-related output signal: output signal enters the safe state
- Impact on the measurement uncertainty:
  - 2 – Moves within the specified SIL error range B
  - 3 – Has no effect

**$\lambda_{DD}$ (Dangerous detected)**
- Dangerous but detectable failure
- Impact on the safety-related output signal: results in a failure mode at the output signal
- Impact on the measurement uncertainty:
  3 – Has no effect

**$\lambda_{DU}$ (Dangerous undetected)**
- Dangerous failure which cannot be detected
- Impact on the safety-related output signal: may be outside the defined error range B
- Impact on the measurement uncertainty:
  4 – May be outside the specified error range

### 3.4.2 Safety measured error

The total deviations with regard to the safety-related current output are composed of:
- A) Measured errors under reference operating conditions: according to TI
- B) Measured errors due to process/installation/ambient conditions: according to TI
- C) Measured errors due to ambient conditions (EMC): ±0.5 % in relation to the span of the safety-related current output
- D) Measured errors due to random component failures (SIL error range): ±2.0 % in relation to the span of the safety-related current output

Strong, pulse-like EMC interference on the power supply line can cause transient (< 1 s) deviations in the output signal (≥ ±1.0 % in relation to the span of the safety-related current output. For this reason, filtering with a time constant of ≥ 1 s should be performed in the downstream logic unit.

### 3.4.3 Systematic faults

Systematic faults are faults for which a cause can be clearly identified that can only be eliminated by modifying the design or the manufacturing process, the method of operation, the operating instructions or other influencing factors.

Failures caused by systematic faults are always reproducible and can be avoided by taking appropriate measures.

The flexible testing of field devices using Heartbeat Verification can support the detection of systematic faults as part of a proof test (see Section 6).

**Examples:**
- **Application-specific faults:**
  Clogged impulse lines, corrosion, diffusion, mechanical stress
  Possible remedy: Heartbeat Monitoring statistical sensor diagnostics
- **Faults during installation, commissioning or maintenance:**
  Possible remedy: Write protection via hardware DIP switch or software wizard safety mode (see Section 4.5.2) with verification of the CRC device configuration checksum.
- **Planning faults:**
  Avoid using unsuitable device configuration for the application.
  Possible remedy: Use Endress +Hauser Applicator to calculate the total performance or diaphragm seal faults.

A0038927

## 3.5 Dangerous undetected failures in this scenario

An incorrect output signal that deviates from the value specified in this manual but is still in the range of 4 to 20 mA, is considered a "dangerous, undetected failure".

## 3.6 Useful lifetime of electric components

A useful lifetime of 20 years applies to the devices described in this manual. The useful lifetime has been determined on the basis of a systematic assessment of all safety-relevant components. Within this time frame, if the approved operating conditions (see IEC 61508-2:2010 Section 7.4.9.5 Note 3) are observed, neither a significant change in the safety-related characteristic values for random failures specified in the Declaration of Conformity nor wear is to be expected.

According to DIN EN 61508-2:2011 Section 7.4.9.5 (national footnote N3) appropriate measures taken by the manufacturer and the operator can extend the useful lifetime.

The useful lifetime can be significantly shorter if the device is operated at temperatures outside specifications.

# 4 Commissioning (Installation and configuration)

## 4.1 Requirements for personnel

The personnel for installation, commissioning, diagnostics and maintenance must fulfill the following requirements:

- Trained, qualified specialists must have a relevant qualification for this specific function and task.
- Personnel must be authorized by the plant owner/operator.
- Be familiar with federal/national regulations.
- Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
- Personnel must follow instructions and comply with general policies.

The operating personnel must fulfill the following requirements:

- Personnel are instructed and authorized according to the requirements of the task by the facility's owner-operator.
- Personnel follow the instructions in this manual.

## 4.2 Installation

The mounting and wiring of the device and the permitted orientations are described in the Operating Instructions pertaining to the device.

Correct installation is a prerequisite for safe operation of the device.

## 4.3 Commissioning

The device can be commissioned using the commissioning wizard. The commissioning procedure is described in the Operating Instructions pertaining to the device.

Prior to operating the device in a safety instrumented system, verification must be performed by carrying out a test sequence as described in **Section 6 Proof testing**.

## 4.4 Operation

The operation of the device is described in the Operating Instructions pertaining to the device.

## 4.5 Device configuration for safety-related applications

### 4.5.1 Adjustment of the measuring point

Measuring point adjustment is described in the Operating Instructions.

The following safety-related parameters must be configured or checked:
- Lower range value output
- Upper range value output
- Simulation
- Current range output
- Failure behavior current output
- Loop current mode
- Measuring mode current output
- Damping
- Output current transfer function
- Sensor pressure range behavior
- Assign PV

For details → GP01149P

The **CRC device configuration** parameter is unique and is built based on the current settings of safety relevant parameters.

CRC device configuration based on current settings of safety relevant parameters.
The CRC device configuration is unique and can be used to detect changes in safety relevant parameter settings.

The following are also relevant for safety:
- Zero adjustment offset
- Lower sensor trim
- Upper sensor trim

### 4.5.2 Device protection

The devices can be protected against external influences as follows:
- Software write protection
  Is set with the **Safety mode** wizard
- Hardware write protection
  Optional via DIP switch (HW lock) on the electronic insert

The application of this method is described below.

### 4.5.3 Device configuration and locking methods

The following operating methods are possible to configure the safety function:
- DTM-based software such as Field Care or Device Care
- MSD-based software SmartBlue (App)
- Operation via display
- EDD-based software such as PDM / FDI /AMS

The safety function can be set in a variety of ways, which are described in detail below:
- Default setting ex works
- Configured on site without the operating menu
- Configuration and locking using the wizard
- Configuration and locking without the wizard

### 4.5.4 Default setting ex works

**Prerequisite**

The customer specified the desired configuration in the order, which was then written to the device during the production process.

A function test must be performed on site by the user before the device may be used in SIL mode. This can be done using one of the procedures described for proof testing (see the "Proof testing" section). It is recommended to approach the measured value for this purpose (test sequence A).

To protect against external influences, the device can be locked using hardware write protection (DIP switch (HW lock) on the electronic insert).

### 4.5.5 Configured on site without the operating menu

Recommended for initial commissioning:
Reset the device according to the Operating Instructions. This resets all parameters to defined values (factory settings or customized settings).

1. Check the position of the DIP switch (HW lock) on the electronic insert, set to "OFF" if necessary.
2. Configure the device as explained in section 9.6.3 of the Operating Instructions.
3. Lock the device using the DIP switch (HW lock) on the electronic insert.

A function test must then be performed before the device may be used in SIL mode. This can be done using one of the procedures described for proof testing (see the "Proof testing" section). It is recommended to approach the measured value for this purpose (test sequence A).

### 4.5.6 Configuration and locking using the wizard

By limiting the possibilities during parameter configuration, this method offers added safety against incorrect settings.

Recommended for initial commissioning:
Reset the device according to the Operating Instructions. This resets all parameters to defined values (factory settings or customized settings).

1. Check the position of the DIP switch (HW lock) on the electronic insert, set to "OFF" if necessary.
2. Carry out the configuration as described in the Operating Instructions, while paying attention to the restrictions (see below). The **Simulation** parameter must be set to **Off** option.
3. Guidance → Safety mode
4. Under SIL preparation, enter "**7 452**" for Enter safety locking code.
   ↳ Locking status = **Temporarily locked** option

A temporary lock is only implemented if all of the following restrictions regarding configuration options are implemented:
- The **Loop current mode** parameter is set to the **Enable** option
- The **Simulation** parameter is set to the **Off** option
- The **Assign PV** parameter is set to the **Pressure** option

5. Perform the **Safety mode** wizard step by step. In the **Locking** wizard, enter "**7 452**" for Enter safety locking code again.
6. Once all the pages have been edited, click on the Finish button to close the wizard.
   ↳ Locking status = Safety-locked option
   Optionally, it is also possible to lock via the DIP switch (HW lock) on the electronic insert.

A function test must then be performed before the device may be used in SIL mode. This can be done using one of the procedures described for proof testing (see the "Proof testing" section). It is recommended to approach the measured value for this purpose (test sequence A).

At the end of the SIL activation sequence, the current **"CRC device configuration" parameter** is stored and the device is safety-locked. If a device is unlocked and locked again, the current **CRC device configuration** parameter is compared with the **Stored CRC device configuration** parameter. If there is no difference in the configuration, the device is safety-locked immediately. If the values deviate from one another, the safety-related parameter settings must be confirmed once again.

If the wizard is canceled, the device is in an unlocked state once again.
▶ Edit all the necessary wizard pages.

### 4.5.7 Configuration and locking without the wizard

A larger number of safety-related parameters can be freely configured. This means that the device can be adapted to difficult applications.

Recommended for initial commissioning:
Reset the device according to the Operating Instructions. This resets all parameters to defined values (factory settings or customized settings).

1. Check the position of the DIP switch (HW lock) on the electronic insert, set to "OFF" if necessary.
2. Carry out the configuration as described in the Operating Instructions. Restriction - the **Simulation** parameter must be set to the **Off** option.
3. Lock the device using the DIP switch (HW lock) on the electronic insert.
4. Check the device settings and document them in a suitable manner. The Fieldcare print function is an easy way to document the device settings.

A function test must then be performed before the device may be used in SIL mode. This can be done using one of the procedures described for proof testing (see the "Proof testing" section). It is recommended to approach the measured value for this purpose (test sequence A).

### 4.5.8 Unlocking device

When safety locking is active on a device, the device is protected against unauthorized operation by means of a locking code and, as an additional option, by means of a write protection switch (DIP switch (HW lock) on the electronic insert). The device must be unlocked in order to change parameters and to reset self-holding diagnostic messages.

1. Check the position of the DIP switch (HW lock) on the electronic insert, set to "OFF" if necessary.
2. Select the "**Guidance** menu → **Safety mode** wizard to call up the wizard.
3. In the **Preparation** wizard, enter "**7 452**" for Enter safety unlocking code.
   ↳ Locking status = **Unlocked**

## 4.6 Parameters and default settings for the SIL mode

The following settings are not permitted for the SIL mode:
- **Simulation** parameter:
  - Pressure
  - Current output
  - Diagnostic event simulation
- **Loop current mode** parameter:
  Disable

# 5 Operation

The behavior during operation and in the event of a fault is described in the Operating Instructions (BA).

## 5.1 Device behavior when switched on

Once switched on, the device runs through a diagnostic phase of approx. 5 s. The current is ≤ 3.6 mA during this phase.

During the diagnostic phase, no communication is possible via the service interface (CDI) or via HART.

## 5.2 Device behavior in safety function demand mode

The device outputs a current value corresponding to the measured value. This value must be monitored and processed further in a connected logic unit.

## 5.3 Safe states

Overpressure or negative pressure in the process are detected by the pressure transmitters. The configured output current "Alarm" or "Warning" is set at the output. This state persists until the application error is resolved and the device can again supply a valid measured value at the current output.

**Malfunction/description**
If a fault is detected, the pressure transmitter sets the configured alarm current (safe state) at the output:
- I ≤ 3.6 mA (low alarm)
  or
- I ≥ 21 mA (high alarm)

The factory setting of the pressure transmitters is I ≤ 3.6 mA (low alarm).

## 5.4 Behavior of device in the event of alarms and warnings

The output current in the event of an alarm can be set to a value of ≤ 3.6 mA or ≥ 21 mA. In some cases (e.g., failure of power supply, a cable open circuit and faults in the current output itself, where the failure current ≥ 21 mA) cannot be set, output currents of ≤ 3.6 mA occur irrespective of the configured failure current.

In some other cases (e.g., short circuit of cabling), output currents of ≥ 21 mA occur irrespective of the configured failure current.

The factory setting for the failure current on HI alarm (**Failure current** parameter) is 22.5 mA

For alarm monitoring, the downstream logic unit must therefore be able to recognize HI alarms (≥ 21 mA) and LO alarms (≤ 3.6 mA).

## 5.5 Alarm and warning messages

The behavior of the device in the event of an alarm and warnings is described in the relevant Operating Instructions.

Correlation between the error code and the current that is output:

**Error code "Fxxx"**
Current output: ≥ 21 mA or ≤ 3.6 mA
Comment: xxx = three-digit number

**Error code ""Mxxx" / "Cxxx" / "Sxxx""**
Current output: as per measured value
Comment: xxx = three-digit number

Overview of output signals depending on the diagnostic state (warning and alarm).

# 6 Proof testing

The safety-related functionality of the device in the SIL mode must be verified during commissioning, when changes are made to safety-related parameters, and also at appropriate time intervals. This enables this functionality to be verified within the entire safety instrumented system. The time intervals must be specified by the operator.

**⚠ CAUTION**

**The safety function is not guaranteed during a proof test**

Suitable measures must be taken to guarantee process safety during the test.

- ▶ The safety-related output signal 4 to 20 mA must not be used for the safety instrumented system during testing.
- ▶ A completed test must be documented; the reports provided in the Appendix can be used for this purpose (see Section 8.2).
- ▶ The operator specifies the test interval and this must be taken into account when determining the probability of failure $PFD_{avg}$ of the sensor system.

If no operator-specific proof testing requirements have been defined, the following is a possible alternative for testing the transmitter depending on the measured variable used for the safety function. The individual proof test coverages (PTC) that can be used for calculation are specified for the test sequences described below.

**NOTICE**

**If there is a device fault before the test, an alarm is output**

- ▶ The cause of the fault must be first eliminated before starting the proof test.

**NOTICE**

**If HW write protection is enabled**

- ▶ Remove HW write protection before carrying out the proof test. If necessary, enable HW write protection again on completion of the proof test.

**NOTICE**

**If SW write protection is enabled**

- ▶ Software write protection must be removed for manual proof testing.

**Overview of the proof tests:**

- Test sequence A
  - Simulate min. and max. alarm current
  - Approach the lower and upper measured value
- Test sequence B
  Simulate min. and max. alarm current

**Note the following for the test sequences:**

- The individual proof test coverages (PTC) that can be used for calculation are specified in the Declaration of Conformity
- The measuring instruments (e.g. ammeter) recommended for the verification should be sufficiently precise
- The test must be carried out in such a way that it verifies the correct operation of the safety-related system in interaction with all of the components

## 6.1 Test sequence A

Proof test procedure:

1. Poll the device identification (check Device tag, Device ID, Serial number, Firmware version and Hardware revision)
2. Read out the setting for the customer-specific **Failure current** parameter (≥ 21 mA) and note it down
3. Simulate the maximum Alarm current (Diagnostics → Simulation → Current output).
4. Check whether the safety instrumented system downstream from the device detects the alarm as expected. Alternatively, measure the output current and compare it with the simulated alarm current.
5. Simulate the minimum Alarm current (Diagnostics → Simulation → Current output)

6. Check whether the safety instrumented system downstream from the device detects the alarm as expected. Alternatively, measure the output current and compare it with the simulated alarm current.
7. Approach process conditions at the end of the measuring range (16 to 20 mA approx.) or apply using pressure reference.
8. Check the safety-related output and assess for accuracy. The result of this step is satisfactory if the output current is within the required accuracy range.
9. Approach process conditions at the start of the measuring range (4 to 8 mA approx.) or apply using pressure reference.
10. Check the safety-related output and assess for accuracy. The result of this step is satisfactory if the output current is within the required accuracy range.

NOTICE

**The proof test has failed if the measured current value deviates from the expected current value by > ±2% (based on the span of the safety-related current output).**

- ▶ For troubleshooting measures, see the Operating Instructions.
- ▶ This test is used to detect 95 % (remaining failure rate $\lambda_{DU}$ = 1 FIT) of dangerous undetected failures (proof test coverage, PTC = 95 %).

## 6.2 Test sequence B

Proof test procedure:

1. Poll the device identification (check Device tag, Device ID, Serial number, Firmware version and Hardware revision)
2. Read out the setting for the customer-specific **Failure current** parameter (≥ 21 mA) and note it down.
3. Simulate the maximum Alarm current (Diagnostics → Simulation → Current output).
4. Check whether the safety instrumented system downstream from the device detects the alarm as expected. Alternatively, measure the output current and compare it with the simulated alarm current
5. Simulate the minimum Alarm current (Diagnostics → Simulation → Current output).
6. Check whether the safety instrumented system downstream from the device detects the alarm as expected. Alternatively, measure the output current and compare it with the simulated alarm current.

NOTICE

**The proof test has failed if the downstream safety instrumented system does not recognize the alarm.**

- ▶ For troubleshooting measures, see the Operating Instructions.
- ▶ This test is used to detect 61 % (remaining failure rate $\lambda_{DU}$ = 10 FIT) of dangerous undetected failures (proof test coverage, PTC = 61 %).

## 6.3 Verification criterion

**If one of the test criteria from the test sequences described above is not fulfilled, the device may no longer be used as part of a safety instrumented system.**

- The purpose of proof-testing is to detect dangerous undetected device failures ($\lambda_{DU}$).
- This test does not cover the impact of systematic faults on the safety function, which must be assessed separately.
- Systematic faults can be caused, for example, by process material properties, operating conditions, build-up or corrosion.
- As part of the visual inspection, for example, ensure that all of the seals and cable entries provide adequate sealing and that the device is not visibly damaged.

# 7 Repair and error handling

## 7.1 Maintenance

Maintenance instructions and instructions regarding recalibration may be found in the Operating Instructions pertaining to the device.

Alternative monitoring measures must be taken to ensure process safety during configuration, proof-testing and maintenance work on the device.

## 7.2 Repair

Repair means restoring functional integrity by replacing defective components.

**Only original Endress+Hauser spare parts may be used for this purpose.**

We recommend that you document the repair and take note of the following:
- Serial number of the device
- Date of the repair
- Type of repair
- Person who performed the repair

Components may be repaired/replaced by the customer's technical staff if **original spare parts** from Endress+Hauser are used (they can be ordered by the end user) and the appropriate installation instructions are followed.

A proof test must always be performed after every repair.

Spare parts are grouped into logical kits with the associated replacement instructions.

Installation Instructions are supplied with the original spare part and can also be accessed in the Download Area at www.endress.com

Send in replaced components to Endress+Hauser for fault analysis.

When returning the defective component, always enclose the "Declaration of Hazardous Material and Decontamination" with the note "Used as SIL device in a safety instrumented system".

Information on returns: http://www.endress.com/support/return-material

## 7.3 Modification

Modifications are changes to SIL devices that are already delivered or installed:
- **Modifications to SIL devices by the user are not permitted because they can impair the functional safety of the device**
- Modifications to SIL devices may be performed onsite at the user's plant following approval by the Endress+Hauser manufacturing center
- Modifications to SIL devices must be performed by personnel authorized to do so by Endress+Hauser
- Only **original spare parts** from Endress+Hauser may be used for modifications
- All modifications must be documented in the Endress+Hauser Device Viewer (www.endress.com/deviceviewer)
- All modifications require a change nameplate or replacement of the original nameplate.

## 7.4 Decommissioning

When decommissioning, the requirements according to IEC 61508-1:2010 section 7.17 must be observed.

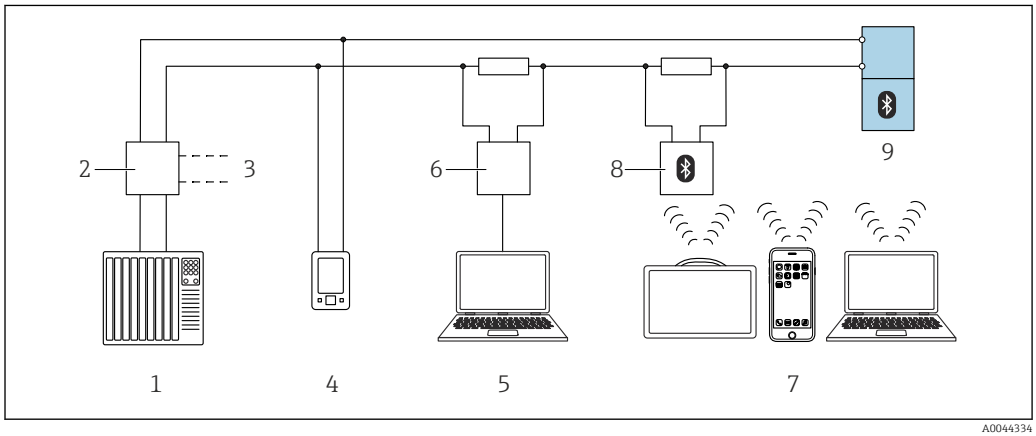
## 7.5 Disposal

If required by the Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), the product is marked with the depicted symbol in order to minimize the disposal of WEEE as unsorted municipal waste. Do not dispose of products bearing this marking as unsorted municipal waste. Instead, return them to the manufacturer for disposal under the applicable conditions.

# 8 Appendix

## 8.1 Structure of the measuring system

### 8.1.1 System components




*2 Options for remote operation via HART protocol (passive)*

1 *Control system (e.g. PLC)*
2 *Transmitter power supply unit, e.g. RN-Series active barrier (with communication resistor)*
3 *Connection for Commubox FXA195 and Field Communicator 475*
4 *TREX Device Communicator*
5 *Computer with operating tool (e.g. FieldCare, DeviceCare, AMS Device Manager, SIMATIC PDM) with COM DTM "CDI Communication TCP/IP"*
6 *Commubox FXA195 (USB), Commubox FXA291 (CDI)*
7 *Tablet with built-in Bluetooth modem / Field Xpert*
8 *VIATOR Bluetooth/HART modem with connecting cable*
9 *Transmitter / transmitter with built-in Bluetooth modem*

An analog signal (4 to 20 mA) in proportion to the pressure is generated in the transmitter. This is sent to a downstream logic unit (e.g. PLC, limit signal transmitter, etc.) where it is monitored to determine whether:
- it exceeds or drops below a predefined value
- it is outside a range to be monitored
- a fault has occurred (e.g. sensor error, interruption or short-circuit of the sensor line, failure of the supply voltage)

For fault monitoring, the logic unit must recognize both HI alarms (≥21 mA) and LO alarms (≤3.6 mA).

### 8.1.2 Description of application as a safety instrumented system

The pressure transmitter is used for the following measuring tasks:
- Absolute pressure and overpressure measurement in gases, vapors or liquids in all areas of process engineering and process measurement technology
- Level, volume or mass measurements in liquids

### 8.1.3 Installation conditions

The installation conditions for various measurements are described in the Technical Information for the device.

Correct installation is a prerequisite for safe operation of the device.

### 8.1.4 Measurement function

The measuring principle and the measurement functions are described in the Operating Instructions for the device.

## 8.2 Commissioning or proof test report

The following device-specific test report acts as a print/master template and can be replaced or supplemented any time by the customer's own SIL reporting and testing system.

### 8.2.1 Test Report - Page 1 -

| Device information |
|---|
| System |
| Device tag |
| Device name/Order code |
| Serial number |
| Firmware version |
| Hardware revision |

| Test information |
|---|
| Company/contact person |
| Performed by |
| Date/time |
| Inspector |

| Verification result | |
|---|---|
| Overall result | |
| ☐ Pass ☑ | ☐ Fail ☒ |

| Notes |
|---|
| |

Date Signature Signature of tester

## 8.2.2 Test Report - Page 2 -

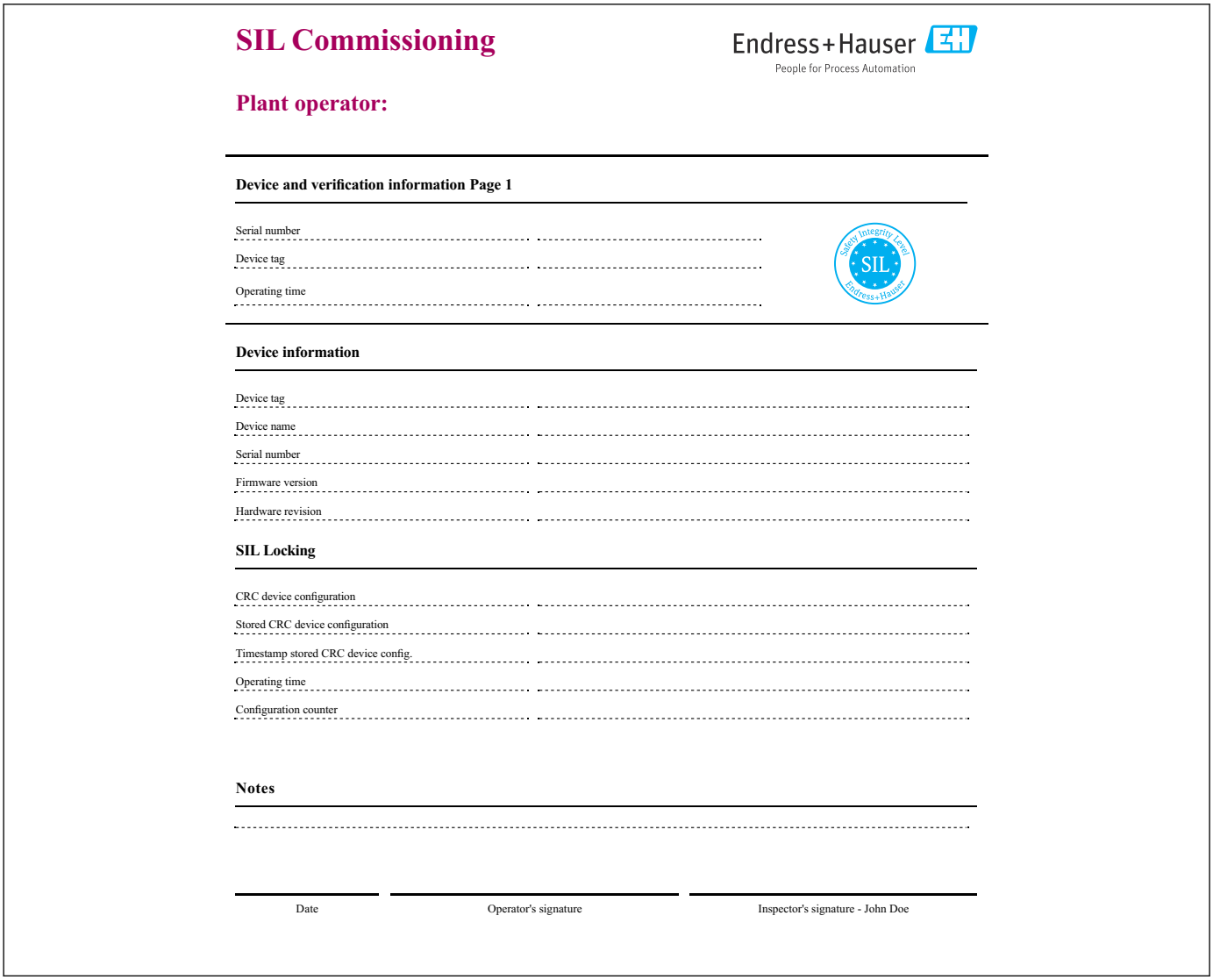
| Device information |
|---|
| System |
| Device tag |
| Serial number |

| Preparation |
|---|
| I have read the warning texts. ☐ Yes |

| Visual inspection |
|---|
| |

| Proof test report | | | |
|---|---|---|---|
| **Test steps** | | | |
| 1. Read out max. Failure current<br>Actual value: | | | mA |
| 2. Simulate max. Failure current<br>Is the alarm detected by the downstream safety instrumented system?<br>☐ Yes ☐ No | | | |
| 3. Simulate min. Failure current<br>Is the alarm detected by the downstream safety instrumented system?<br>☐ Yes ☐ No | | | |
| 4. Approach upper measured value (approx. 16 to 20 mA) or apply it via pressure reference<br>Actual value: | | | mA |
| 5. Measure Current at output<br>Actual value: | | | mA |
| 6. Result (Max. toler. deviation < +/-2%), with reference to the span of the safety-related current output? | ☐ Yes | ☐ No | |
| 7. Approach lower measured value (approx. 4 to 8 mA) or apply it via pressure reference<br>Actual value: | | | mA |
| 8. Measure Current at output<br>Actual value: | | | mA |
| 9. Result (Max. toler. deviation < +/-2%), with reference to the span of the safety-related current output? | ☐ Yes | ☐ No | |

### 8.2.3 Commissioning Test Report - Page 1 -



**SIL Commissioning**

Endress+Hauser
People for Process Automation

**Plant operator:**

**Device and verification information Page 1**

Serial number .....

Device tag .....

Operating time .....

**Device information**

Device tag .....

Device name .....

Serial number .....

Firmware version .....

Hardware revision .....

**SIL Locking**

CRC device configuration .....

Stored CRC device configuration .....

Timestamp stored CRC device config. .....

Operating time .....

Configuration counter .....

**Notes**

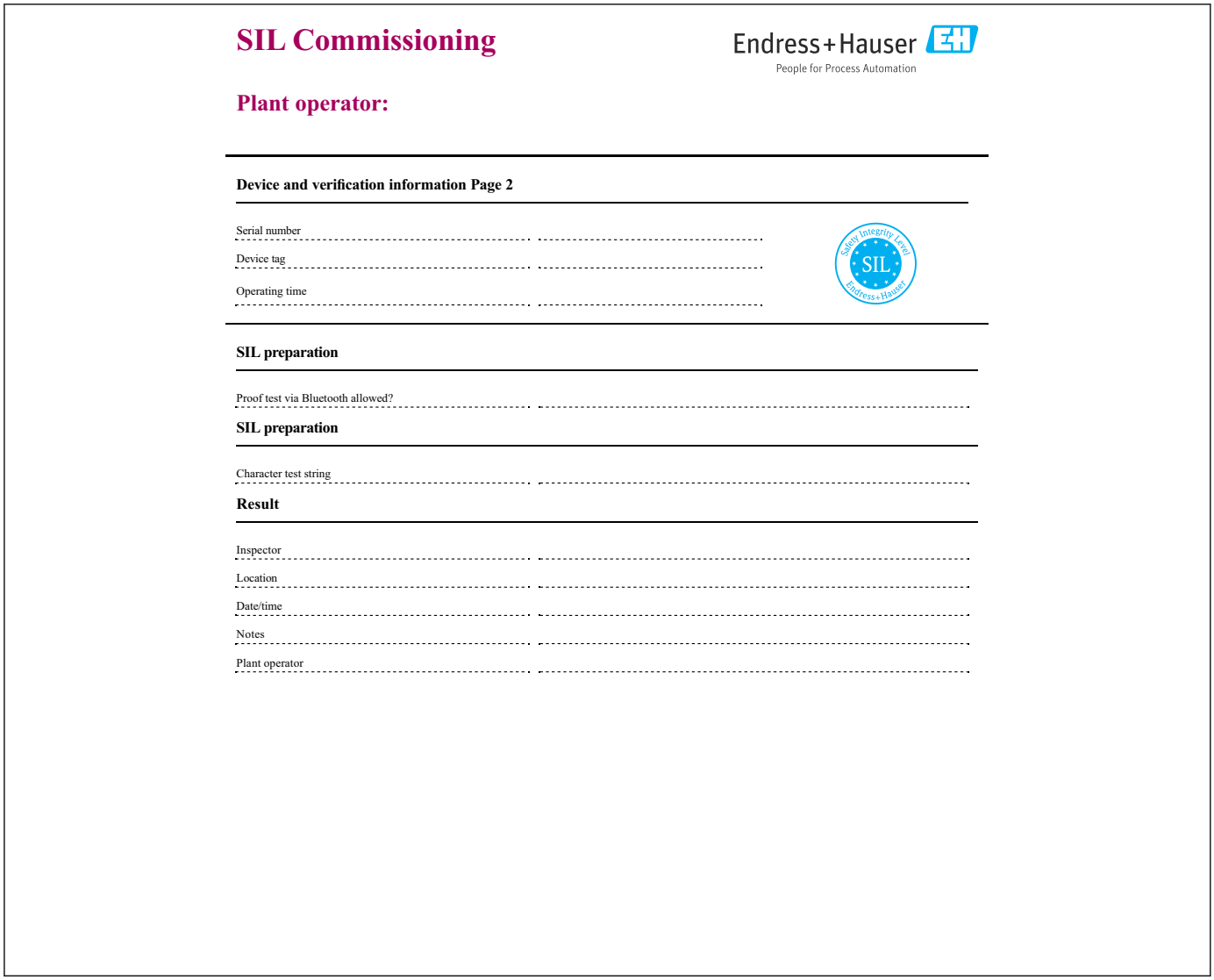
.....

Date | Operator's signature | Inspector's signature - John Doe

A0045207

3 *Example of a commissioning report using the wizard - Page 1 -*

### 8.2.4 Commissioning Test Report - Page 2 -



**SIL Commissioning**

Endress+Hauser
People for Process Automation

**Plant operator:**

**Device and verification information Page 2**

Serial number

Device tag

Operating time

**SIL preparation**

Proof test via Bluetooth allowed?

**SIL preparation**

Character test string

**Result**

Inspector

Location

Date/time

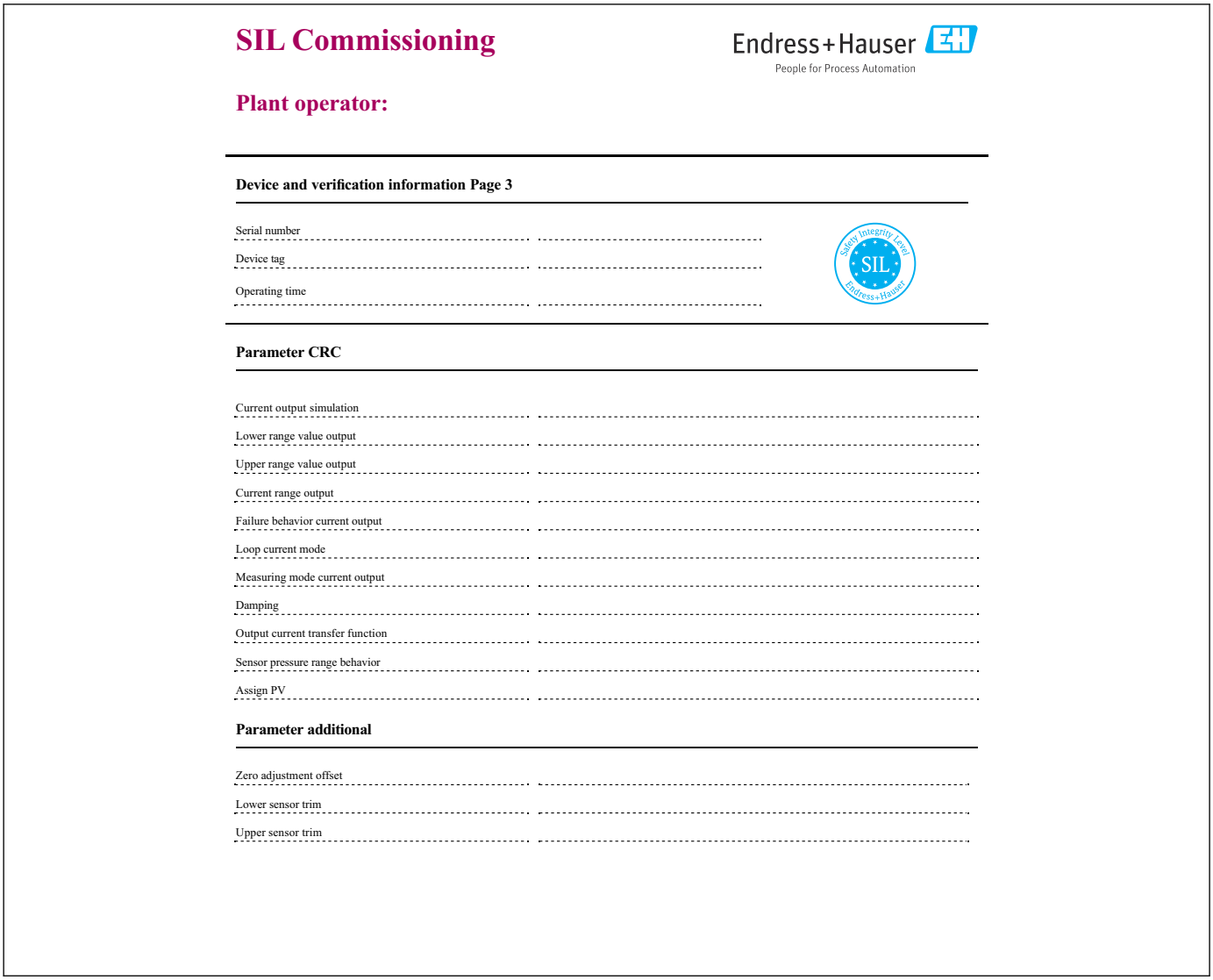
Notes

Plant operator

A0045208

4 *Example of a commissioning report using the wizard - Page 2 -*

### 8.2.5 Commissioning Test Report - Page 3 -



**SIL Commissioning**

Endress+Hauser
People for Process Automation

**Plant operator:**

**Device and verification information Page 3**

Serial number .....

Device tag .....

Operating time .....

**Parameter CRC**

Current output simulation .....

Lower range value output .....

Upper range value output .....

Current range output .....

Failure behavior current output .....

Loop current mode .....

Measuring mode current output .....

Damping .....

Output current transfer function .....

Sensor pressure range behavior .....

Assign PV .....

**Parameter additional**

Zero adjustment offset .....

Lower sensor trim .....

Upper sensor trim .....

A0045209

*5 Example of a commissioning report using the wizard - Page 3 -*

## 8.3 Version history

**FY01025P; Version 01.20**
- Firmware version: 01.00.zz (zz: any double number)
- Hardware version: 01.00.ww (ww: any double number) or from date of device delivery
- Changes:
  First version

**FY01025P; Version 02.22**
- Firmware version: 01.00.zz (zz: any double number)
- Hardware version: 01.00.ww (ww: any double number) or from date of device delivery
- Changes:
  Safety-related characteristic values improved

**FY01025P; Version 03.24**
- Firmware version: 01.00.zz (zz: any double number)
- Hardware version: 01.00.ww (ww: any double number) or from date of device delivery
- Changes:
  Declaration of Conformity

**FY01025P; Version 04.24**
- Firmware version: 01.01.zz (zz: any double number)
- Hardware version: 01.00.ww (ww: any double number) or from date of device delivery
- Changes:
  - Software update
  - Useful lifetime extended to 20 years


www.addresses.endress.com

Endress+Hauser

People for Process Automation