

# Konformitätserklärung

KE\_FS\_Pmass200\_d.docx



## Konformitätserklärung

Funktionale Sicherheit nach IEC 61508:2010  
Beiblatt 1 / NE130 Formblatt B1

**Endress+Hauser Flowtec AG, Kägenstrasse 7, CH-4153 Reinach**

erklärt als Hersteller, dass das Durchflussmessgerät

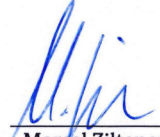
### Promass 200

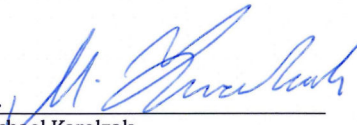
für den Einsatz in sicherheitsrelevanten Anwendungen nach IEC61508:2010 geeignet ist.

In sicherheitsrelevanten Anwendungen gemäß IEC 61508 und IEC 61511 sind die Angaben des Handbuchs zur Funktionalen Sicherheit zu beachten.

Reinach, 29 . Mai. 2015

Endress+Hauser Flowtec AG

  
\_\_\_\_\_  
Marcel Ziltener  
Direktor Controlling

  
i.V. \_\_\_\_\_  
Michael Karolzak  
Project Manager Functional Safety

SIL\_00481\_01.21

## Sicherheitstechnische Kenngrößen

| Allgemein  |  |
|--|--|
| Gerätebezeichnung und zulässige Ausführungen   | 8A2B**... (Promass A 200)<br>8E2B**... (Promass E 200)<br>8E2C**... (Promass E 200)<br>8F2B**... (Promass F 200)   |
|  | Bestellmerkmal "Ausgang":<br><ul style="list-style-type: none"> <li>▪ Option A "4-20mA HART"</li> <li>▪ Option B "4-20mA HART, Imp./ Freq./Schaltausg."</li> <li>▪ Option C "4-20mA HART, 4-20mA"</li> </ul> Bestellmerkmal "Weitere Zulassung":<br>Option <b>LA</b> "SIL"   |
| Sicherheitsbezogenes Ausgangssignal  | 4...20 mA  |
| Fehlerstrom  | ≤ 3,6 mA oder ≥ 21 mA  |
| Bewertete Messgröße / Funktion   | Überwachung Masse- oder Volumenfluss oder Dichte   |
| Sicherheitsfunktion(en)  | Min., Max., Bereich  |
| Gerätetyp gem. IEC 61508-2   | <input type="checkbox"/> Typ A <input checked="" type="checkbox"/> Typ B   |
| Betriebsart  | <input checked="" type="checkbox"/> Low Demand Mode <input checked="" type="checkbox"/> High Demand Mode <input type="checkbox"/> Continuous Mode <sup>1)</sup>  |
| Gültige Hardware-Version (Hauptelektronik)   | Ab Auslieferungsdatum 01.03.2014   |
| Gültige Firmware-Version   | Ab 01.04.zz (HART; ab Auslieferungsdatum 01.06.2015)   |
| Sicherheitshandbuch  | SD00147D   |
| Art der Bewertung (nur 1 Variante wählbar)   | <input checked="" type="checkbox"/> Vollständige entwicklungsbegleitende HW/SW Bewertung inkl. FMEDA und Änderungsprozess nach IEC 61508-2, 3<br><input type="checkbox"/> Bewertung über Nachweis der Betriebsbewährung HW/SW inkl. FMEDA und Änderungsprozess nach IEC 61508-2, 3<br><input type="checkbox"/> Auswertung von Felddaten HW/SW zum Nachweis "Frühere Verwendung/Prior Use" gem. IEC 61511<br><input type="checkbox"/> Bewertung durch FMEDA gem. IEC 61508-2 für Geräte ohne Software |
| Bewertung durch (inkl. Berichtsnr. + FMEDA Datenquelle)                                    | TÜV Rheinland Industrie Service GmbH – Zertifikat Nr. 968/EZ 504.01/12   |
| Prüfunterlagen   | Entwicklungsdokumente, Testreports, Datenblätter   |
| SIL-Integrität   |  |
| Systematische Sicherheitsintegrität  | <input type="checkbox"/> SIL 2 fähig <input checked="" type="checkbox"/> SIL 3 fähig   |
| Hardware Sicherheitsintegrität   | Einkanliger Einsatz (HFT = 0) <input checked="" type="checkbox"/> SIL 2 fähig <input type="checkbox"/> SIL 3 fähig   |
|  | Mehrkanliger Einsatz (HFT ≥ 1) <input type="checkbox"/> SIL 2 fähig <input checked="" type="checkbox"/> SIL 3 fähig  |
| FMEDA  |  |
| Sicherheitsfunktion(en)  | Min., Max., Bereich  |
|  | Option <b>A, B</b> Option <b>C</b>   |
| $\lambda_{DU}^{2)}$  | 89 FIT    73 FIT   |
| $\lambda_{DD}^{2)}$  | 1168 FIT    1010 FIT   |
| $\lambda_{SU}^{2)}$  | 1105 FIT    1720 FIT   |
| $\lambda_{SD}^{2)}$  | 1374 FIT    1374 FIT   |
| SFF - Safe Failure Fraction  | 97 %    98 %   |
| PFD <sub>avg</sub> für T <sub>1</sub> = 1 Jahr <sup>3)</sup><br>(einkanalige Architektur)  | $3,9 \cdot 10^{-4}$ $3,2 \cdot 10^{-4}$  |
| PFD <sub>avg</sub> für T <sub>1</sub> = 5 Jahre <sup>3)</sup><br>(einkanalige Architektur) | $1,9 \cdot 10^{-3}$ $1,6 \cdot 10^{-3}$  |
| PFH  | $4,5 \cdot 10^{-8}$ $3,7 \cdot 10^{-8}$  |

|  |          |           |
|--|----------|-----------|
| PTC <sup>4)</sup>  | Bis 98 % |           |
| MTBF <sub>tot</sub> <sup>5)</sup>  | 47 Jahre | 40 Jahre  |
| Diagnose-Testintervall <sup>6)</sup>   | 30 min   |           |
| Fehlerreaktionszeit <sup>7)</sup>  | 30 s     |           |
| Prozesssicherheitszeit <sup>8)</sup>   | 50 h     |           |
| Empfohlenes Prüflintervall T <sub>1</sub>  | 5 Jahre  |           |
| MTTF <sub>d</sub> <sup>9)</sup>  | 89 Jahre | 105 Jahre |
| <b>Bemerkung</b>   |          |           |
| Das Messgerät wurde entwickelt für den Gebrauch im "Low Demand"- und "High Demand"-Betrieb.  |          |           |
| <b>Erklärung</b>   |          |           |
| <input checked="" type="checkbox"/> Unser firmeninternes Qualitätsmanagement stellt die Information von zukünftig bekannt werdenden sicherheitsrelevanten systematischen Fehlern sicher. |          |           |

- 1) Kein kontinuierlicher Betrieb gemäß IEC 61508: 2011 (Kapitel 3.5.16)
- 2) FIT = Failure In Time, Anzahl der Ausfälle pro 10<sup>9</sup> h
- 3) Gültig für gemittelte Umgebungstemperaturen bis zu 40 °C (104 °F) gemäß allgemeinem Standard für SIL-fähige Geräte.
- 4) PTC = Proof Test Coverage (Diagnoseaufdeckungsgrad von Gerätefehlern bei manueller Wiederholungsprüfung)
- 5) Dieser Wert berücksichtigt alle Ausfallarten der Elektronikkomponenten gemäß Siemens SN29500
- 6) In dieser Zeit werden alle Diagnosefunktionen mindestens 1x ausgeführt.
- 7) Maximale Zeit zwischen Fehlererkennung und Fehlerreaktion.
- 8) Die Prozesssicherheitszeit beträgt Diagnose-Testintervall \* 100 (Berechnung nach IEC 61508).
- 9) MTTF<sub>d</sub> nach ISO 13849/IEC 62061 schließt auch Soft-Errors ein (sporadische Bitfehler in Datenspeichern).

**Safety-related characteristic values**

| General  |   |
|--|---|
| Device designation and permitted versions  | 8A2B**... (Promass A 200)<br>8E2B**... (Promass E 200)<br>8E2C**... (Promass E 200)<br>8F2B**... (Promass F 200)  |
|  | Order code for "Output":<br><ul style="list-style-type: none"> <li>▪ Option A "4-20mA HART"</li> <li>▪ Option B "4-20mA HART, pul./freq./switch output"</li> <li>▪ Option C "4-20mA HART, 4-20mA"</li> </ul> Order code for "Additional approval":<br>Option LA "SIL" |
| Safety-related output signal   | 4 to 20 mA  |
| Failure current  | ≤ 3.6 mA or ≥ 21 mA   |
| Assessed measured variable/function  | Monitoring of mass flow, volume flow or density   |
| Safety function(s)   | Min., Max., Range   |
| Device type according to IEC 61508-2   | <input type="checkbox"/> Type A <input checked="" type="checkbox"/> Type B  |
| Operating mode   | <input checked="" type="checkbox"/> Low Demand Mode <input checked="" type="checkbox"/> High Demand Mode <input type="checkbox"/> Continuous Mode <sup>1)</sup>   |
| Valid hardware version (main electronics)  | From delivery date March 1, 2014  |
| Valid firmware version   | 01.04.zz and higher (HART; from delivery date June 1, 2015)   |
| Safety manual  | SD00147D  |
| Type of assessment<br>(only 1 version can be selected)   | <input checked="" type="checkbox"/> Complete HW/SW assessment in the context of development including FMEDA and change process according to IEC 61508-2, 3  |
|  | <input type="checkbox"/> Assessment of evidence for proven-in-use HW/SW including FMEDA and change process according to IEC 61508-2, 3  |
|  | <input type="checkbox"/> Analysis of HW/SW field data for evidence of "prior use" according to IEC 61511  |
|  | <input type="checkbox"/> Assessment by FMEDA according to IEC 61508-2 for devices without software  |
| Assessment by (including report no. + FMEDA data source)                                       | TÜV Rheinland Industrie Service GmbH – Certificate No. 968/EZ 504.01/12   |
| Test documents   | Development documents, test reports, data sheets  |
| SIL integrity  |   |
| Systematic safety integrity  | <input type="checkbox"/> SIL 2 capable <input checked="" type="checkbox"/> SIL 3 capable  |
| Hardware safety integrity  | Single-channel service (HFT = 0) <input checked="" type="checkbox"/> SIL 2 capable <input type="checkbox"/> SIL 3 capable   |
|  | Multi-channel service (HFT ≥ 1) <input type="checkbox"/> SIL 2 capable <input checked="" type="checkbox"/> SIL 3 capable  |
| FMEDA  |   |
| Safety function(s)   | Min., Max., Range   |
|  | Option A, B    Option C   |
| $\lambda_{DU}$ <sup>2)</sup>   | 89 FIT    73 FIT  |
| $\lambda_{DD}$ <sup>2)</sup>   | 1168 FIT    1010 FIT  |
| $\lambda_{SU}$ <sup>2)</sup>   | 1105 FIT    1720 FIT  |
| $\lambda_{SD}$ <sup>2)</sup>   | 1374 FIT    1374 FIT  |
| SFF - Safe Failure Fraction  | 97 %    98 %  |
| PFD <sub>avg</sub> for T <sub>1</sub> = 1 year <sup>3)</sup><br>(single-channel architecture)  | $3.9 \cdot 10^{-4}$ $3.2 \cdot 10^{-4}$   |
| PFD <sub>avg</sub> for T <sub>1</sub> = 5 years <sup>3)</sup><br>(single-channel architecture) | $1.9 \cdot 10^{-3}$ $1.6 \cdot 10^{-3}$   |
| PFH  | $4.5 \cdot 10^{-8}$ $3.7 \cdot 10^{-8}$   |
| PTC <sup>4)</sup>  | Up to 98 %  |

|  |          |           |
|--|----------|-----------|
| MTBF <sub>tot</sub> <sup>5)</sup>  | 47 years | 40 years  |
| Diagnostic test interval <sup>6)</sup>   | 30 min   |           |
| Fault response time <sup>7)</sup>  | 30 s     |           |
| Process safety <sup>8)</sup>   | 50 h     |           |
| Recommended test interval T <sub>1</sub>   | 5 years  |           |
| MTTF <sub>d</sub> <sup>9)</sup>  | 89 years | 105 years |
| <b>Note</b>  |          |           |
| The measuring device has been developed for use in "Low Demand" and "High Demand" mode.  |          |           |
| <b>Explanation</b>   |          |           |
| <input checked="" type="checkbox"/> Our in-house quality management system saves information on safety-related systematic errors that will become known in the future. |          |           |

- 1) No continuous operation as per IEC 61508: 2011 (section 3.5.16)
- 2) FIT = Failure In Time, number of failures per 10<sup>9</sup> h
- 3) Valid for averaged ambient temperatures up to 40 °C (104 °F) in accordance with general standard for devices with SIL capabilities.
- 4) PTC = Proof Test Coverage (diagnostic coverage achieved by device failure detection during manual proof testing)
- 5) This value takes into account all failure types of the electronic components as per Siemens SN29500
- 6) All diagnostic functions are carried out at least once during this time.
- 7) Maximum time between fault detection and fault response.
- 8) The process safety is the diagnostics test interval \* 100 (calculation as per IEC 61508).
- 9) MTTF<sub>d</sub> according to ISO 13849/IEC 62061 also includes soft errors (sporadic bit errors in data memories).