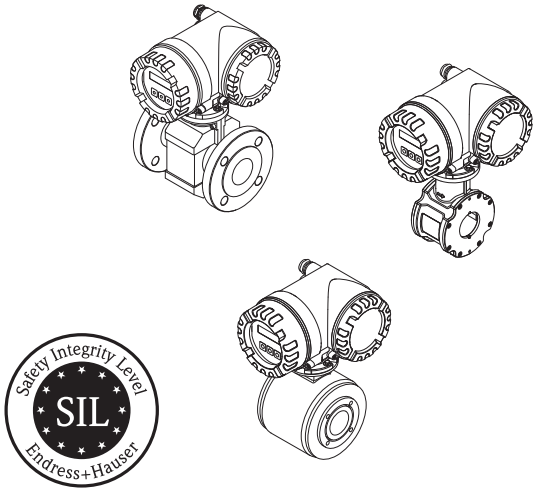
SD00115D/06/DE/15.14
71249501

gültig ab Version
V 02.00.00 (Gerätesoftware)

Handbuch zur Funktionalen Sicherheit
Proline Promag 50, 53

Magnetisch-induktives Durchflussmessgerät mit 4...20 mA Ausgangssignal



Anwendungsbereich
Überwachung des maximalen und/oder minimalen Durchflusses in Anlagen, die den besonderen Anforderungen der Sicherheitstechnik nach IEC/EN 61508 und IEC/EN 61511-1 genügen sollen.

Das Messgerät erfüllt die Anforderungen an
- Funktionale Sicherheit gemäß IEC/EN 61508 und IEC/EN 61511-1
- Explosionsschutz (je nach Version)
- Elektromagnetische Verträglichkeit nach EN 61326-3-2 und NAMUR-Empfehlung NE 21

Ihre Vorteile
- Einsatz für Durchflussüberwachung (Min., Max., Bereich) bis SIL 2 – unabhängig beurteilt (Functional Assessment) durch exida.com nach IEC/EN 61508 und IEC/EN 61511-1
- Kontinuierliche Messung
- Nahezu unabhängige Messung von Produkteigenschaften
- Permanente Selbstüberwachung
- Einfache Installation und Inbetriebnahme
- Wiederholungsprüfung ohne Ausbau des Messgeräts möglich

Endress+Hauser
People for Process Automation

Inhaltsverzeichnis

SIL Konformitätserklärung

Endress+Hauser
People for Process Automation

Antoine Simon
Endress+Hauser Flowtec AG
Kägenstrasse 7, 4153 Reinach

SIL Konformitätserklärung Promag 50/Promag 53
Funktionale Sicherheit eines Durchflussmessgerätes nach IEC 61508/IEC 61511

Endress+Hauser Flowtec AG, Kägenstrasse 7, 4153 Reinach
erklärt als Hersteller, dass die Durchflussmessgeräte

Promag 50 (4…20 mA) und Promag 53 (4…20 mA)

für den Einsatz in einer sicherheitsrelevanten Anwendung bis einschließlich SIL 2 entsprechend IEC 61511-1 und IEC 61508 geeignet sind, wenn die Installation konform zum Safety Manual ist, und wenn die Sicherheitshinweise beachtet werden.

Die FMEDA Analyse der sicherheitskritischen und gefährlichen Zufallsfehler liefert unter Annahme einer mindestens alle 24 Monate erfolgenden Funktionsprüfung in der ungünstigsten der getesteten Konfigurationen folgende Parameter:

SIL (Sicherheitslevel)	:	2
HFT (Hardware Fehlertoleranz)	:	0 [1)]
Gerätetyp	:	Type B (Komplexe Komponente)
SFF (Anteil sicherheitsgerichteter Fehler)	:	>76%
PFD_{AVG} (Mittlere Versagenswahrscheinlichkeit bei Anforderung)[2)]	:	$\leq 1{,}29 \cdot 10^{-3}$ p.a.

Fehlerraten nach IEC 61508, basiert auf der „worst case“ Konfiguration:

λ_{du} (Gesamtausfallrate für gefährliche unerkannte Ausfälle)	:	$295 \cdot 10^{-9}$/h (295 FIT)
λ_{dd} (Gesamtausfallrate für gefährliche erkannte Ausfälle)	:	$756 \cdot 10^{-9}$/h (756 FIT)
λ_{su} (Gesamtausfallrate für sichere unerkannte Ausfälle)	:	$265 \cdot 10^{-9}$/h (265 FIT)
λ_{sd} (Gesamtausfallrate für sichere erkannte Ausfälle)	:	$0 \cdot 10^{-9}$/h (0 FIT)

1) gemäß Kapitel 11.4 der IEC 61511-1
2) Die PFD_{AVG} Werte sind auch nach ISA S84.01 innerhalb des für SIL 2 definierten Bereichs gültig.

Im Rahmen des Nachweises der Betriebsbewährtheit wurde das Gerät einschließlich der Software (ab Verstärkerversion V2.00.00, und IO-Modul Software 1.04.00) und das Änderungswesen beurteilt.

Reinach, 05.10.2006

Endress+Hauser Flowtec AG
FEE/SA

SIL2-50-53-Conformity-de.pdf

Allgemeines

Darstellung eines Sicherheitssystems (Schutzfunktion)

Mit den nachfolgenden Tabellen wird der erreichbare Safety Integrity Level (SIL) oder die Anforderungen bezüglich der "mittleren Versagenswahrscheinlichkeit bei Anforderung" (PFD_{AVG}), der "Hardware Fehlertoleranz" (HFT) und dem "Anteil sicherheitsgerichteter Ausfälle" (SFF) an das Sicherheitssystem bestimmt. Die spezifischen Werte für das Messsystem Promag finden Sie in den Tabellen im Anhang.

Allgemein gelten folgende zulässige Versagenswahrscheinlichkeiten der gesamten Sicherheitsfunktion in Abhängigkeit zum SIL für Systeme, die auf Anforderungen – z.B. Überschreiten eines definierten max. Durchflusses – reagieren müssen (Quelle: IEC 61508, Teil 1):

SIL	PFD_{AVG}
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Die nachfolgende Tabelle zeigt den erreichbaren SIL abhängig vom Wahrscheinlichkeitsanteil sicherheitsgerichteter Ausfälle und der Hardware Fehlertoleranz des gesamten Sicherheitssystems für Systeme vom Typ B (komplexe Bauelemente, Definition siehe IEC 61508, Teil 2):

SFF	HFT		
	0	1 (0)[1)]	2 (1)[1)]
< 60 %	nicht erlaubt	SIL 1	SIL 2
60 % ... < 90 %	SIL 1	**SIL 2**	SIL 3
90 % ... < 99 %	SIL 2	SIL 3	
≥ 99 %	SIL 3		

1) Nach IEC 61511-1 (Kapitel 11.4.4) kann die HFT um 1 reduziert werden (Werte in Klammern), wenn die eingesetzten Geräte folgende Bedingungen erfüllen:
- das Gerät ist betriebsbewährt
- es können am Gerät nur prozessrelevante Parameter geändert werden (z.B. Messbereich, ...)
- die Veränderung der prozessrelevanten Parameter ist geschützt (z.B. Passwort, Jumper, ...)
- die Funktion erfordert weniger als SIL 4

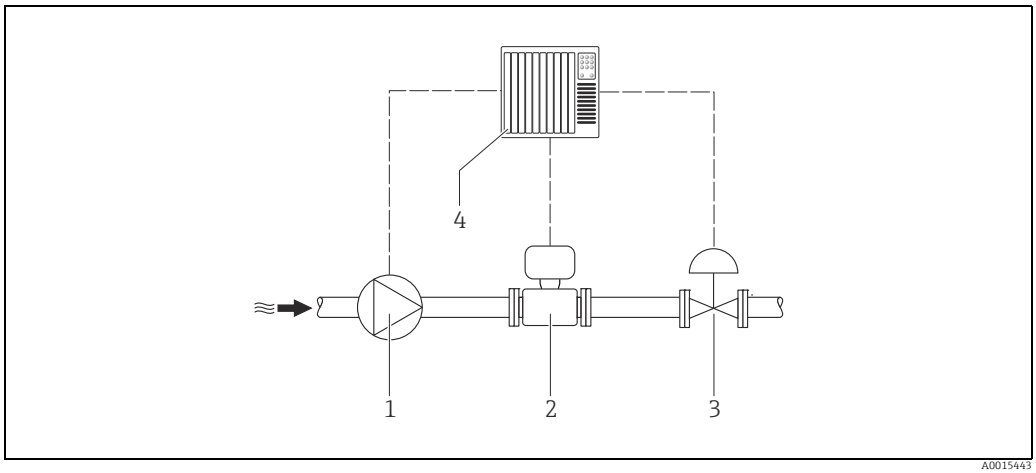
Das Promag Messsystem erfüllt diese Bedingungen.

Das Messgerät darf in PLT-Schutzfunktionen mit einkanaliger Architektur für SIL 2 oder mit diversitär redundanter Architektur für SIL 3 eingesetzt werden. Eine Verwendung in PLT-Schutzfunktionen mit homogenen redundanten Auswahlschaltungen für SIL 3 ist ausgeschlossen.

Hinweis!
Allgemeine Informationen über Funktionale Sicherheit (SIL) sind erhältlich unter: www.de.endress.com/SIL und in der Kompetenzbroschüre CP002Z "Funktionale Sicherheit in der Prozess-Instrumentierung zur Risikoreduzierung" (Verfügbar im Download-Bereich der Endress+Hauser Internetseite: www.endress.com → Download → Dokumentationscode: CP002Z).

Aufbau des Messsystems mit Promag 50, 53

Systemkomponenten



A0015443

Systemkomponenten

1 Pumpe
2 Messgerät
3 Ventil
4 Automatisierungssystem

Im Messumformer wird ein dem Durchfluss proportionales, analoges Signal (4–20 mA) erzeugt, das einem nachgeschalteten Automatisierungssystem zugeführt wird und dort auf das Überschreiten oder Unterschreiten eines vordefinierten Grenzwerts überwacht wird.

Hinweis!
- Das sicherheitsbezogene Signal ist das analoge Ausgangssignal 4–20 mA des Messgeräts. Alle Sicherheitsfunktionen beziehen sich ausschließlich auf den Stromausgang 1.
- Das Gerät muss vor unbefugtem Zugriff geschützt sein → siehe Abschnitt "Verriegelung" (→ 🖹 7).
- Das Anwendungsprogramm im Sicherheits-Automatisierungssystem ist so gestaltet, dass "Fail High"- und "Fail Low"-Ausfälle unabhängig vom Effekt (sicher oder gefährlich) von der Sicherheitsfunktion detektiert werden.
- Wird beim Messgerät Promag 53 die Kommunikation zusätzlich über das HART-Protokoll ausgeführt, muss der HART-Schreibschutz aktiviert sein → siehe Abschnitt "Verriegelung" (→ 🖹 7).

Die ermittelten Kennwerte (siehe Anhang) gelten ausschließlich für den 4–20 mA Stromausgang der folgenden Varianten:
- Promag 50***–**********(*)
  (*) = Bestelloption für Ein- /Ausgänge: A / W / D/ S / T
- Promag 53***–**********(*)
  (*) = Bestelloption für Ein- /Ausgänge: A / B / C / L / M / S / T / 2 / 4

Angaben für die Sicherheitsfunktion

Die verbindlichen Einstellungen und Angaben für die Sicherheitsfunktion gehen aus dem Kapitel "Einstellungen und Installationshinweise" (→ 🖹 6) sowie aus dem Anhang (→ 🖹 15) hervor. Die Reaktionszeit des Messsystems beträgt ≤ 2 s. Erst danach beginnt die Alarmverzögerung der Überwachungsfunktion.

Hinweis!
Die Zeit vom Auftreten eines Ausfalls bis zu dessen Beseitigung (MTTR) wird mit 8 Stunden angesetzt.

Mitgeltende Gerätedokumentationen

Für das Messsystem müssen folgende Dokumentationen vorhanden sein:

Gerätetyp	Betriebsanleitung	Beschreibung der Gerätefunktionen
Promag 50	BA00046D/06	BA00049D/06
Promag 53	BA00047D/06	BA00048D/06

In diesen Dokumentationen befinden sich auch Angaben über Anwendungsgrenzen und Umgebungsbedingungen sowie die funktionalen Spezifikationen des Stromausgangs.
Für Messgeräte mit Explosionsschutz-Zulassungen sind außerdem die entsprechenden Sicherheitshinweise der zugehörigen Ex-Dokumentation (XA) zu beachten.

Einstellungen und Installationshinweise

Installationshinweise

Hinweise zur korrekten Installation des Messgeräts entnehmen Sie der mitgelieferten Betriebsanleitung (BA) → siehe "Mitgeltende Gerätedokumentationen" (→ 5).

Eignung des Messgeräts

Die Nennweite des Messgeräts gemäß den in der Applikation zu erwartenden Durchflüssen sorgfältig auswählen. Der maximale Durchfluss im Betrieb darf den spezifizierten Maximalwert des Aufnehmers nicht überschreiten. Weiterhin wird empfohlen, in sicherheitsrelevanten Anwendungen den Grenzwert zur Überwachung eines minimalen Durchflusses nicht kleiner als 5 % des spezifizierten Maximalwerts des Aufnehmers zu wählen.
Den anwendungsgemäßen Einsatz des Messgeräts und dabei die Eigenschaften des Messstoffs und der Umgebungsbedingungen berücksichtigen. Alle Hinweise auf kritische Prozesssituationen und Installationsverhältnisse aus den Gerätedokumentationen beachten.
Anwendungen vermeiden, die Ablagerungen oder Korrosion im Messrohr verursachen.
Für einphasige, flüssige Messstoffe mit wasserähnlichen Eigenschaften müssen im Allgemeinen keine besonderen Anforderungen berücksichtigt werden.

Hinweis!
Weitere Informationen sind bei Ihrer Endress+Hauser Vertriebsstelle erhältlich.

Einstellhinweise

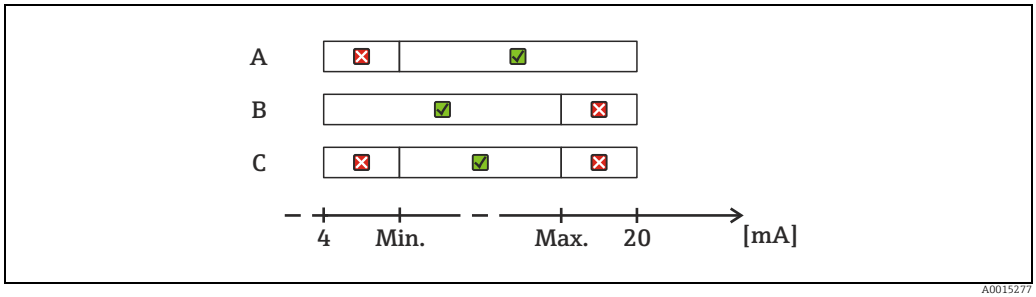
Das Messgerät kann in PLT Schutzeinrichtungen auf verschiedene Arten konfiguriert werden:
- Via Vor-Ort-Bedienung (LCD-Anzeige)
- Via HART-Handbediengerät DXR 375
- Via PC (Fernbedienung) über eine Service- und Konfigurationssoftware (z.B. "FieldCare")

Über die genannten Tools können auch Angaben zur Software- und Hardware-Revision des Gerätes abgefragt werden. Weitere Hinweise zu den Einstellungen sind den entsprechenden Betriebsanleitungen zu entnehmen → siehe "Mitgeltende Gerätedokumentationen" (→ 5).

Überwachungsmöglichkeiten

In Schutzeinrichtungen kann das Messgerät zur Volumenfluss-Überwachung (Min., Max., Bereich) eingesetzt werden.

Hinweis!
Der sichere Betrieb des Geräts setzt eine ordnungsgemäße Installation voraus.



A0015277

Überwachungsmöglichkeiten in Schutzeinrichtungen

A Min.-Alarm
B Max.-Alarm
C Bereichsüberwachung

☒ *= Auslösen der Schutzfunktion*
☑ *= Zulässiger Betriebszustand*

In folgenden Tabelle sind die Einstellungen angegeben, die zum Einsatz des Messgeräts in einer sicherheitsrelevanten Applikation notwendig sind. Diese Einstellungen beziehen sich grundsätzlich auf den 4–20 mA Ausgangswert des Stromausgangs, der dem Durchflusswert entspricht.

Gruppe	Funktionsname in der Gruppe	Einstellmöglichkeiten bei Verwendung des Promass für eine Sicherheitsfunktion
STROMAUSGANG	ZUORDNUNG STROMAUSGANG	Volumenfluss
STROMAUSGANG	STROMBEREICH	– 4–20 mA (.....): Alle Einstellmöglichkeiten, in denen der Stromausgang auf 4–20 mA konfiguriert wird. – 0...20 mA: Einstellung ist nicht zulässig. **Promag 50** Alle Einstellmöglichkeiten 4–20 mA mit HART-Kommunikation sind nicht zulässig. **Promag 53** Alle Einstellmöglichkeiten 4–20 mA mit HART-Kommunikation sind nur dann zulässig, wenn der HART-Schreibschutz aktiviert ist (→ 🖹 7, Abschnitt "Verriegelung")
STROMAUSGANG	FEHLERVERHALTEN	– Min. Stromwert – Max. Stromwert
STROMAUSGANG	SIMULATION STROM	Aus
SYSTEMPARAMETER	MESSWERTUNTERDRÜCKUNG	Aus
ÜBERWACHUNG	ZUORDNUNG SYSTEMFEHLER	Aus (die Zuordnung von Hinweis- und Fehlermeldungen darf nicht verändert werden)
ÜBERWACHUNG	ALARM VERZÖGERUNG	0...20 s
SIMULATION SYSTEM	SIMULATION FEHLERVERHALTEN	Aus
SIMULATION SYSTEM	SIMULATION MESSGRÖSSE	Aus

Eine ausführliche Beschreibung der Messgerätefunktionen entnehmen Sie der zugehörigen Dokumentation "Beschreibung der Gerätefunktionen" → siehe "Mitgeltende Gerätedokumentationen" (→ 🖹 5).

Verriegelung

Zum Schutz der prozessrelevanten Parameter vor Änderung muss die Software verriegelt werden. Dies geschieht mit Hilfe eines durch den Anwender wählbaren Codes.

Softwareverriegelung für lokale Bedienung	
Funktion KUNDENCODE	Frei wählbare Codenummer (außer 0)

Promass 53:
Bei Verwendung der HART-Kommunikation muss der HART-Schreibschutz aktiviert werden. Dies geschieht mit Hilfe einer Steckbrücke auf der I/O-Platine. Das korrekte Vorgehen zur Aktivierung des HART-Schreibschutzes entnehmen Sie der entsprechenden Betriebsanleitung → siehe "Mitgeltende Gerätedokumentationen" (→ 🖹 5).

Einstellhinweise zur Auswerteeinheit

Am nachfolgenden Grenzwertgeber (Automatisierungssystem) muss der ermittelte Grenzwert (mA-Wert entsprechend dem gewünschten Maximal- und/oder Minimalwert des Durchflusses) eingegeben werden. Bei allen Abgleich- und Einstellvorgängen ist gemäß der zugehörigen Betriebsanleitung vorzugehen → siehe "Mitgeltende Gerätedokumentationen" (→ 🖹 5).

Verhalten bei Störungen

Das Verhalten im Betrieb und bei Störungen wird in der Betriebsanleitung des Messgerätes beschrieben → siehe "Mitgeltende Gerätedokumentationen" (→ 🖹 5).

Hinweis!

- **Reparatur:** Die Reparatur der Geräte darf grundsätzlich nur durch Endress+Hauser durchgeführt werden.
  Erfolgt die Reparatur von anderer Seite, können die sicherheitstechnischen Funktionen nicht mehr gewährleistet werden.
  Ausnahme: Der Austausch von modularen Komponenten durch Originalersatzteile darf durch qualifiziertes Personal des Kunden vorgenommen werden, wenn dieses Personal durch Endress+Hauser hierfür geschult wurde.
- Bei Ausfall eines SIL gekennzeichneten Endress+Hauser Geräts, das in einer Schutzeinrichtung betrieben wurde, ist Endress+Hauser unter sil@endress.com mit Angabe des Gerätetyps, der Seriennummer und Art des Ausfalls zu informieren.
  Der Anwender beschreibt dem Hersteller den Ausfall und mögliche Auswirkungen in Form einer detaillierten Mitteilung. Zusätzlich erfolgt ein Informationsfluss, ob es sich um einen gefährlichen oder nicht direkt ermittelbaren Ausfall handelt.
- Bei Ausfall eines SIL-gekennzeichneten Endress+Hauser-Geräts, das in einer Schutzfunktion betrieben wurde, ist bei der Rücksendung des defekten Geräts die "Erklärung zur Kontamination und Reinigung" mit dem entsprechenden Hinweis "Einsatz als SIL-Gerät in Schutzeinrichtung" beizulegen.

Informationen zur Gebrauchsdauer elektrischer Bauteile

Die zugrunde gelegten Ausfallraten elektrischer Bauteile gelten innerhalb der Gebrauchsdauer gemäß IEC/EN 61508-2, Abschnitt 7.4.7.4, Anmerkung, Hinweis 3.

Hinweis!
Nach DIN EN 61508-2, Hinweis NA4 sind durch entsprechende Maßnahmen des Herstellers und Betreibers längere Gebrauchsdauern zu erreichen.

Wiederholungsprüfung

Wiederholungsprüfung (proof test) des Messsystems

Sicherheitsfunktionen sind in angemessenen Zeitabständen auf ihre Funktionsfähigkeit zu überprüfen. Das Prüfintervall ist vom Betreiber festzulegen und bei der Ermittlung der Versagenswahrscheinlichkeit PFD_{avg} des Messaufnehmersystems zu berücksichtigen.

Hinweis!
Der anzusetzende Wert von PFD_{avg} hängt bei einkanaliger Architektur nach folgender Formel vom Diagnose-Deckungsgrad der Wiederholungsprüfung (PTC = Proof Test Coverage) und der vorgesehenen Lebensdauer (LT = Lifetime) ab:

$$PFD_{avg} \approx \lambda_{du} \cdot [PTC/2 \cdot T_i + (1 - PTC)/2 \cdot LT]$$

A0015275

Die Funktionsprüfung ist so durchzuführen, dass die einwandfreie Funktion der Sicherheitseinrichtung im Zusammenwirken aller Komponenten nachgewiesen wird. Jede Prüfung ist vollständig zu dokumentieren.
Zur Überprüfung der Schutzfunktion (Min., Max., Bereich) muss zunächst die Genauigkeit des Messwerts überprüft werden. Hierzu müssen die eingestellten Grenzwerte angefahren werden, worauf die Schutzfunktion einschließlich des Aktors ansprechen muss. Zur Überprüfung der Schutzfunktion Bereich genügt die Überprüfung der Genauigkeit der Messwerte.
Während der Wiederholungsprüfung müssen zur Gewährleistung der Prozesssicherheit alternative überwachende Maßnahmen ergriffen werden.

Eine Wiederholungsprüfung des Geräts kann in folgenden Schritten durchgeführt werden:

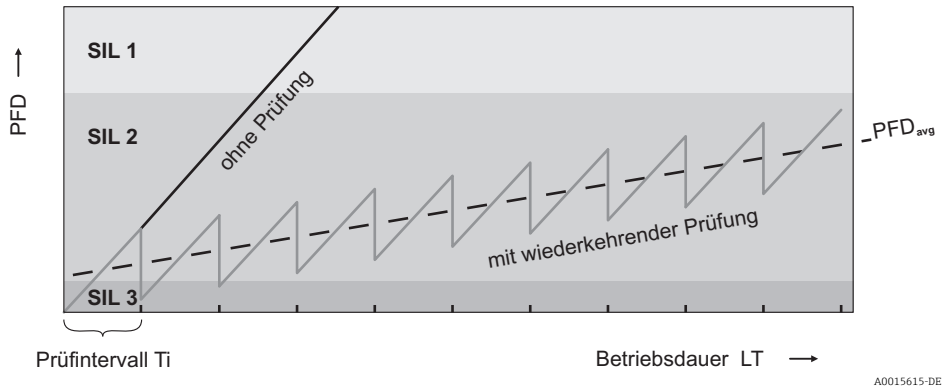
1. **Überprüfung des digitalen Messwerts**
   Je nach zu überwachender Messgröße und verfügbarem Equipment ist eine der folgenden Überprüfungen durchzuführen:
   a. Prüfablauf A – Überprüfung des digitalen Messwerts mit einer Kalibrieranlage
      Volumenfluss
      Eine Rekalibrierung des Messgeräts wird mit einer nach ISO 17025 zertifizierten Kalibrieranlage durchgeführt. Dies kann im eingebauten Zustand mit einer mobilen Kalibrieranlage oder nach Ausbau auf einer Werkskalibrieranlage erfolgen. Die betragsmäßige Abweichung des gemessenen Durchflusses vom Sollwert darf die in der Betriebsanleitung aufgeführte maximale Messabweichung nicht überschreiten.

      Hinweis!
      Weitere Informationen zu Standardverfahren für die Vor-Ort-Kalibrierung von Durchflussmessgeräten sind bei Ihrer Endress+Hauser Vertriebsstelle erhältlich.

   b. Prüfablauf B – Überprüfung des digitalen Messwerts mit Hilfe des eingebauten Summenzählers
      Volumenfluss
      Ein geeichtes Messgefäß wird mit dem Medium bei einem Durchfluss gefüllt, der dem zu überwachenden Grenzwert näherungsweise entspricht. Die Veränderung des Volumens im Messgefäß wird vor und nach der Füllung abgelesen und mit dem im Messgerät eingebauten Summenzähler verglichen. Die betragsmäßige Abweichung darf die in der Betriebsanleitung aufgeführte maximale Messabweichung nicht überschreiten. Im Falle einer Bereichsüberwachung ist diese Überprüfung für den oberen und unteren Grenzwert separat durchzuführen.

   c. Prüfablauf C – Überprüfung des digitalen Messwerts mit Fieldcheck
      Volumenfluss
      Verifikation des Messgeräts im eingebauten Zustand mit Fieldcheck gemäß Betriebsanleitung BA00067D/06. Fieldcheck zeigt das Prüfungsergebnis (Bestanden/Nicht Bestanden) automatisch an.
      Dieser Prüfablauf kann ohne Ausbau des Durchflussmessgeräts erfolgen und vereinfacht die wiederkehrende Prüfung. Durch den hohen Diagnosedeckungsgrad werden > 90 % der verdeckten Fehler erkannt, wodurch die mittlere Versagenswahrscheinlichkeit PFD_{AVG} geringer ansteigt als ungeprüft (→ nachfolgende Grafik). Die mittlere Versagenswahrscheinlichkeit PFD_{AVG} kann mit dessen Formel (→ 🖹 9) und der vorgesehenen Gebrauchsdauer t abgeschätzt werden.

      Zusammen mit dem Softwarepaket FieldCare können die Testergebnisse in eine Datenbank übernommen, ausgedruckt und als Nachweis für Behörden weiter verwendet werden.



Einkanalige Systemarchitektur 1oo1

2. **Überprüfung des 4–20 mA Stromausgangs**
   Der Stromausgang des Messgeräts ist mit Hilfe der im Bedienmenü verfügbaren Stromsimulation (fester Stromwert) nacheinander auf die Werte 3,6 mA, 4,0 mA, 20,0 mA und 22,0 mA einzustellen und mit den Messwerten eines externen geeichten Strommessgeräts zu vergleichen.

3. **Überprüfung der Schutzfunktion**
   Durch Ausgabe geeigneter Stromwerte auf der 4–20 mA Schnittstelle per Stromsimulation (knapp unterhalb und oberhalb des Schaltpunkts) ist das korrekte Ansprechen der Schutzfunktion inklusive Aktor zu überprüfen. Im Falle einer Bereichsüberwachung ist diese Überprüfung für den oberen und unteren Grenzwert separat durchzuführen.

4. Abschluss der Wiederholungsprüfung
   Den 4–20 mA Stromausgang auf Messwertausgabe schalten (wenn notwendig).

Hinweis!
Die Wiederholungsprüfung ist nur abgeschlossen, wenn die Schritte 1...4 durchgeführt wurden.
Mit den beschriebenen Prüfabläufen 1a bis 1b können mindestens 98 %, mit Prüfablauf 1c mindestens 90 %, der unerkannten gefährlichen Fehler entdeckt werden. Ist eines der Prüfkriterien der beschriebenen Prüfabläufe nicht erfüllt, darf das Messgerät nicht mehr als Teil einer Schutzeinrichtung eingesetzt werden.
Der Einfluss systematischer Fehler auf die Sicherheitsfunktion wird durch die Prüfung nicht abgedeckt und ist gesondert zu betrachten. Systematische Fehler können beispielsweise durch Messstoffeigenschaften, Betriebsbedingungen, Ansatzbildung oder Korrosion verursacht werden.

Exida Management Summary

FMEDA and Proven-in-use Assessment

Project:
Electromagnetic Flow Measuring System PROMAG 50/53

Customer:
Endress+Hauser Flowtec AG
Reinach
Switzerland

Contract No.: E+H 06/02-03
Report No.: E+H 06/02-03 R039
Version V1, Revision R1, October 2006
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the electromagnetic flow measuring system PROMAG 50/53 with 4..20 mA HART® output and software version 02.00.00. The statements made in this report are also valid for further software versions as long as the assessed IEC 61508 modification process is considered. Any changes are under the responsibility of the manufacturer. Table 1 gives an overview of the different types that belong to the considered electromagnetic flow measuring system PROMAG 50/53.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview

Version	Type	Commodul	Options
V1	50***-**********W	C03	Current
	50***-**********A	C03	Current + Frequency
	50***-**********D	C03	Current + Frequency + Status output + Status input
V2	53***-**********C	C05	Current + Frequency + 2 * Relays
	53***-**********L	C05	Current + 2 * Relays + Status input
	53***-**********M	C05	Current + 2*Frequency + Status input
	53***-**********2	C05	Current + Current2 + Frequency + Relay
	53***-**********4	C05	Current + Frequency + Current input + Relay
V3	53***-**********A	C06	Current + Frequency
	53***-**********B	C06	Current + Frequency + 2 * Relays
V4	53***-**********S	C07	Current active + Frequency passive
V5	53***-**********T	C07	Current passive + Frequency passive

For safety applications only the 4..20 mA current output was considered. All other possible output variants or electronics are not covered by this report. The different devices can be equipped with or without display.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part.

For a SIL 2 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-03.

The electromagnetic flow measuring system PROMAG 50/53 is considered to be a Type B[1] sub-system with a hardware fault tolerance of 0.

Type B sub-systems with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

As the electromagnetic flow measuring system PROMAG 50/53 is supposed to be a proven-in-use sub-system, an assessment of the hardware with additional proven-in-use demonstration was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 a hardware fault tolerance of 0 is sufficient for SIL 2 sub- systems being Type B sub-systems and having a SFF of 60% to < 90%.

The proven-in-use investigation was based on field return data collected and analyzed by Endress+Hauser Flowtec AG.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 the device is suitable to be used, as a single device, for SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

Endress+Hauser Flowtec AG performed a qualitative analysis of the mechanical parts of the electromagnetic flow measuring system PROMAG 50/53 (see [D7]). This analysis was used by *exida* to calculate the failure rates of the sensor elements using *exida*'s experienced-based data compilation for the different components of the sensor elements (see [R1]). The results of the quantitative analysis were used for the calculations described in sections 5.1 to 5.6.

Assuming that the application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled.

Table 2: Summary for the worst case version – Failure rates [2]

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**756**
Fail dangerous detected (internal diagnostics or indirectly [3])	598
Fail high (detected by the logic solver)	7
Fail low (detected by the logic solver)	140
Annunciation detected	11
Fail Dangerous Undetected	**295**
Fail dangerous undetected	285
Annunciation undetected	10
No Effect	**265**
Not part	**194**

[1] Type B sub-system: "Complex" sub-system (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

[2] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

[3] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

Table 3: Summary for the worst case version – IEC 61508 Failure rates

λ_{SD}	λ_{SU} [4]	λ_{DD}	λ_{DU}	SFF	DC_S [5]	DC_D [3]
0 FIT	265 FIT	756 FIT	295 FIT	77%	0%	71%

Table 4: Summary for the worst case version – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,29E-03	PFD_{AVG} = 6,43E-03	PFD_{AVG} = 1,28E-02

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in green ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in red ( ) mean that the calculated PFD_{AVG} values do not fulfill the requirements for SIL 2 according to table 2 of IEC 61508-1.

The failure rates listed above do not include failures resulting from incorrect use of the electromagnetic flow measuring system PROMAG 50/53, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the electromagnetic flow measuring system PROMAG 50/53 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 5.1 to 5.6. along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the electromagnetic flow measuring system PROMAG 50/53 (see Appendix 3).

[4] Note that the SU category includes failures that do not cause a spurious trip

[5] DC means the diagnostic coverage (safe or dangerous).

Anhang (Sicherheitstechnische Kennwerte)

Einleitende Bemerkungen

Die Promag Durchfluss-Messsysteme werden, je nach Bestellstruktur, mit unterschiedlichen Signaleingängen und -ausgängen ausgeliefert. Gleichartige Elektronikmodule sind aus Gründen der Übersicht in "Kategorien" zusammengefasst.

Hinweis!
- Für jede dieser "Kategorien" werden die sicherheitstechnischen Kennwerte separat beschrieben → siehe Abschnitte "Kategorie 1...7". Die dort aufgeführten Tabellen beinhalten alle wichtigen Kennwerte. Dabei gelten die Werte für alle Einsatzmöglichkeiten.
- Die angegebenen Ausfallraten beziehen sich auf die Ausfallraten der Siemens Norm SN29500 bei einer Umgebungstemperatur von +40 °C (+104 °F).

Messsystem / Elektronik Bestellstruktur	Aus- und Eingänge	Kategorie → 🗎 16
Promag 50		
50*** – *************W**	Stromausg.	**1**
50*** – *************A**	Stromausg. / Frequenzausg.	**1**
50*** – *************D**	Stromausg. / Frequenzausg. / Statusausg. / Statuseing.	**1**
50*** – *************S**	Stromausg. aktiv (Ex i) / Frequenzausg. passiv (Ex i)	**6**
50*** – ***********T	Stromausg. passiv (Ex i) / Frequenzausg. passiv (Ex i)	**7**
Promag 53		
53*** – *************C**	Stromausg. / Frequenzausg. / Relais / Relais 2	2
53*** – *************L**	Stromausg. / Relais / Relais 2 / Statuseing.	**2**
53*** – *************M**	Stromausg. / Frequenzausg. / Frequenzausg. 2 / Statuseing.	**2**
53*** – *************2**	Stromausg. / Stromausg. 2 / Frequenzausg. / Relais	**2**
53*** – *************4**	Stromausg. / Frequenzausg. / Relais / Stromeing.	**2**
53*** – *************A**	Stromausg. / Frequenzausg.	**3**
53*** – *************B**	Stromausg. / Frequenzausg. / Relais / Relais 2	**3**
53*** – *************S**	Stromausg. aktiv (Ex i) / Frequenzausg. passiv (Ex i)	**4**
53*** – *************T**	Stromausg. passiv (Ex i) / Frequenzausg. passiv (Ex i)	**5**

- ATEX II2G/D, FM/CSA Cl.1 Div.1, TIIS und NEPSI sind verfügbare Optionen für Promag H/P/W
- ATEX II3G/D ist verfügbare Option für Promag E/H/P/W
- FM/CSA Cl.1 Div.2 ist verfügbare Option für Promag D/E/H/L/P/W

Anmerkungen zum Begriff "Gefährliche unerkannte Ausfälle"

Als "gefährliche unerkannte Ausfälle" gelten solche Zustände, bei denen der Prozess auf eine Anfrage nicht antwortet (d.h. das Messgerät zeigt nicht das vordefinierte Fehlerverhalten) oder bei denen das Ausgangssignal mehr als die spezifizierte Gesamtmessunsicherheit vom wahren Messwert abweicht. Detaillierte Angaben zur Gesamtmessunsicherheit finden Sie in der Betriebsanleitung, Kapitel "Messgenauigkeit".

Dabei wird von folgenden Annahmen ausgegangen:
- Die Ausfallraten sind konstant, Abnutzungsmechanismen werden nicht betrachtet.
- Ausfallfortpflanzung ist nicht relevant.
- Das HART-Protokoll wird während des normalen Messbetriebes nur zum Auslesen von Daten verwendet.
- Die Wiederherstellungszeit nach einem sicheren Ausfall beträgt 8 Stunden.
- Die Testzeit des Automatisierungssystems, um auf einen detektierten Ausfall zu reagieren, beträgt eine Stunde.
- Alle Module werden im "Low Demand Mode" betrieben.
- Nur der Stromausgang 1 wird für sicherheitsrelevante Anwendungen verwendet.
- Ausfallraten der externen Spannungsversorgung werden nicht betrachtet.

- Die "Stress Levels" sind Durchschnittswerte für eine industrielle Umgebung und sind vergleichbar mit der "Ground Fixed"-Klassifizierung des MIL-HDBK-217F. Alternativ ist die angenommene Umgebung ähnlich IEC 60654-1, Class C (geschützter Einbauort) mit Temperaturgrenzen innerhalb der Herstellerangaben und einer Durchschnittstemperatur über eine längere Zeitperiode von +40 °C (+104 °F) für den Messumformer (Transmitter). Die Feuchtigkeit wird innerhalb der Herstellerspezifikation angenommen.
- Nur die beschriebenen Versionen werden für Sicherheitsanwendungen verwendet.
- Da die optionale Anzeige nicht Teil der Sicherheitsfunktion ist, wird die Ausfallrate des Displays nicht in den Berechnungen berücksichtigt.
- Das Anwendungsprogramm im Sicherheits-Automatisierungssystem ist so gestaltet, dass "Fail High"- und "Fail Low"-Ausfälle unabhängig vom Effekt (sicher oder gefährlich) von der Sicherheitsfunktion detektiert werden.

Kategorien

- SIL (Sicherheitslevel) = 2
- HFT (Hardware-Fehlertoleranz gemäss IEC 61511-1 Kapitel 11.4) = 0
- Gerätetyp = Type B (Komplexe Komponente)

Kategorie	SFF[1)]	PFD_{AVG}			λ_{du}	λ_{dd}	λ_{su}	λ_{sd}
		1 Jahr	2 Jahre	5 Jahre				
1	76,68 %	$\leq 1{,}27 \cdot 10^{-3}$	$\leq 2{,}54 \cdot 10^{-3}$	$\leq 6{,}35 \cdot 10^{-3}$	291 FIT	705 FIT	253 FIT	0 FIT
2	77,58 %	$\leq 1{,}29 \cdot 10^{-3}$	$\leq 2{,}58 \cdot 10^{-3}$	$\leq 6{,}45 \cdot 10^{-3}$	295 FIT	756 FIT	265 FIT	0 FIT
3	76,89 %	$\leq 1{,}28 \cdot 10^{-3}$	$\leq 2{,}56 \cdot 10^{-3}$	$\leq 6{,}40 \cdot 10^{-3}$	292 FIT	711 FIT	260 FIT	0 FIT
4	81,06 %	$\leq 1{,}25 \cdot 10^{-3}$	$\leq 2{,}50 \cdot 10^{-3}$	$\leq 6{,}25 \cdot 10^{-3}$	285 FIT	854 FIT	365 FIT	0 FIT
5	80,29 %	$\leq 1{,}21 \cdot 10^{-3}$	$\leq 2{,}42 \cdot 10^{-3}$	$\leq 6{,}05 \cdot 10^{-3}$	277 FIT	847 FIT	283 FIT	0 FIT
6	80,29 %	$\leq 1{,}24 \cdot 10^{-3}$	$\leq 2{,}50 \cdot 10^{-3}$	$\leq 6{,}25 \cdot 10^{-3}$	285 FIT	854 FIT	365 FIT	0 FIT
7	80,29 %	$\leq 1{,}20 \cdot 10^{-3}$	$\leq 2{,}42 \cdot 10^{-3}$	$\leq 6{,}05 \cdot 10^{-3}$	277 FIT	847 FIT	283 FIT	0 FIT

1) Safe Failure Fraction

www.addresses.endress.com

Endress+Hauser

People for Process Automation