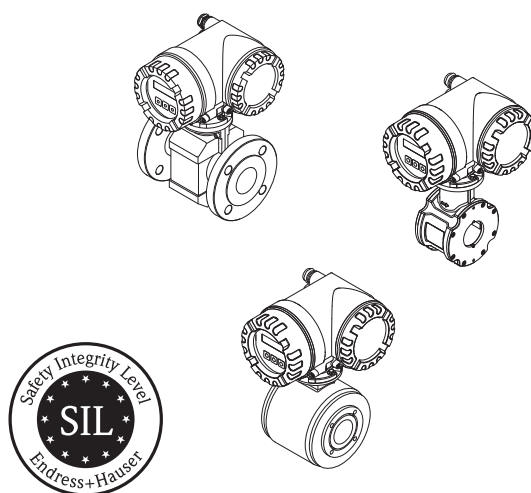


Podręcznik dotyczący bezpieczeństwa funkcjonalnego **Proline Promag 50, 53**

Przepływomierz elektromagnetyczny
wersja z wyjściem 4...20 mA



Zastosowanie

Monitorowanie przepływu maksymalnego i/lub minimalnego w systemach, które muszą spełniać wymagania szczegółowe bezpieczeństwa określone w normie PN-EN 61508 i PN-EN 61511-1.

Przyrząd spełnia wymagania dotyczące:

- Bezpieczeństwa funkcjonalnego zgodnie z PN-EN 61508/61511-1
- Ochrony przeciwwybuchowej (w zależności od wersji)
- Kompatybilności elektromagnetycznej zgodnie z normą PN-EN 61326-3-2 i zalecaniami NAMUR NE 21

Korzyści

- Zastosowanie w systemach monitorowania przepływu zapewniających poziom nienaruszalności bezpieczeństwa funkcjonalnego do SIL 2 – weryfikowanym przez niezależną instytucję exida.com zgodnie z normą IEC/EN 61508 i IEC/EN 61511-1
- Ciągły pomiar
- Pomiar jest praktycznie niezależny od własności medium
- Ciągła autodiagnostyka obwodów wewnętrznych
- Łatwa instalacja i uruchomienie
- Możliwość wykonywania testu kontrolnego bez konieczności demontażu urządzenia pomiarowego

Spis treści

Deklaracja zgodności SIL	3
Wstęp	4
Opis systemu bezpieczeństwa (funkcji bezpieczeństwa)	4
Konfiguracja układu pomiarowego z przetwornikiem Promag 50, 53	5
Elementy układu pomiarowego	5
Parametry funkcji bezpieczeństwa	5
Dokumentacja uzupełniająca	5
Ustawienia i instrukcje montażu	6
Instrukcje montażu	6
Instrukcje konfiguracji	6
Opcje monitorowania	6
Blokada zapisu danych konfiguracyjnych	7
Instrukcje konfiguracji jednostki logicznej	7
Odpowiedź pomiarowa i reakcja przyrządu na stan błędu	8
Informacje na temat użytecznego cyklu życia podzespołów elektrycznych	8
Test kontrolny	9
Test kontrolny układu pomiarowego	9
Streszczenie dla kierownictwa opracowane przez Exida	11
Dodatek (parametry związane z bezpieczeństwem funkcjonalnym)	15
Uwagi wstępne	15
Kategorie	16

Deklaracja zgodności SIL



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

SIL Declaration of Conformity Promag 50/Promag 53
Functional Safety of a flow measuring device according to IEC 61508/IEC 61511

Endress+Hauser Flowtec AG, Kägenstrasse 7, 4153 Reinach
declares as manufacturer, that the flow measuring devices

Promag 50 (4...20 mA) and Promag 53 (4...20 mA)

are suitable for the use in a safety instrumented system up to SIL 2 according to IEC 61511-1 und IEC 61508 if the installation is conform to the safety manual and if enclosed safety instructions are observed.

The FMEDA with analysis of the safety critical and dangerous faults provides under the assumption of a functional test cycle of two years the following parameters for the worst case of the tested configurations:

SIL (Safety Integrity Level)	:	2
HFT (Hardware Fault Tolerance)	:	0 ¹⁾
Device Type	:	Type B (complex component)
SFF (Safe failure fraction)	:	>76%
PFDAVG (Average Probability of Failure on Demand) ²⁾	:	$\leq 1.29 \cdot 10^{-3}$ p.a.

Failure rates according to IEC 61508, based on the worst case configuration:

λ_{du} (failure rate dangerous undetected failures)	:	$295 \cdot 10^{-9}/h$ (295 FIT)
λ_{dd} (failure rate dangerous detected failures)	:	$756 \cdot 10^{-9}/h$ (756 FIT)
λ_{su} (failure rate safe undetected failures)	:	$265 \cdot 10^{-9}/h$ (265 FIT)
λ_{sd} (failure rate safe detected failures)	:	$0 \cdot 10^{-9}/h$ (0 FIT)

1) According to clause 11.4 of IEC 61511-1

2) The PFDAVG values are also within the range for SIL 2 according to ISA S84.01.

The assessment of the proven-in-use demonstration covers the device and its software (as of software version V2.00.00 (amplifier), and 1.04.00 (communication module)) including the modification process.

Reinach, 05.10.2006

Endress+Hauser Flowtec AG
FEE/SA

Wstęp

Opis systemu bezpieczeństwa (funkcji bezpieczeństwa)

W poniższych tabelach podano poziomy nienaruszalności bezpieczeństwa (SIL) i odpowiednie wartości "średniego prawdopodobieństwa uszkodzenia niebezpiecznego funkcji bezpieczeństwa w trybie pracy na rzadkie przywołanie" (PFD_{AVG}), oraz wymagania dotyczące "Tolerancji defektów sprzętu" (HFT) i "Udziału uszkodzeń bezpiecznych" (SFF) dla systemu bezpieczeństwa. Specyficzne wartości dla układu pomiarowego z przetwornikiem Promag podano w tabelach w Dodatku.

Zależność poziomów nienaruszalności bezpieczeństwa SIL od średniego prawdopodobieństwa niezadziałania funkcji bezpieczeństwa wykonywanej przez przepływomierz, który pracuje w trybie na rzadkie przywołanie, np. przekroczenie określonej maksymalnej wartości przepływu - (Źródło: norma PN-EN 61508-2):

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

W poniższej tabeli podano poziomy nienaruszalności bezpieczeństwa SIL oraz odpowiednie wartości udziału uszkodzeń bezpiecznych i tolerancji defektów sprzętu dla systemu bezpieczeństwa typu B (urządzeń złożonych), którego definicję podano w normie IEC 61508-2:

SFF	HFT		
	0	1 (0) ¹⁾	2 (1) ¹⁾
< 60%	Nie dopuszcza się	SIL 1	SIL 2
60 % do < 90 %	SIL 1	SIL 2	SIL 3
90 % do < 99 %	SIL 2	SIL 3	
≥ 99 %	SIL 3		

- 1) Zgodnie z normą PN-EN 61511-1 (rozdział 11.4.41), wartość HFT można zmniejszyć o jedną jednostkę (wartości w nawiasach) jeśli używane urządzenia spełniają następujące wymagania:
- Urządzenie jest sprawdzone w użyciu
 - Tylko w samym urządzeniu można zmieniać ważne parametry procesu (np. zakres pomiarowy, ...)
 - Zmiana ważnych parametrów procesu jest zabezpieczona (np. hasłem, zworką, ...)
 - Poziom bezpieczeństwa funkcjonalnego funkcji bezpieczeństwa musi być niższy od SIL 4

Te warunki są spełnione dla układu pomiarowego wykorzystującego przetworniki Promag.

Przetwornik może być stosowany w pętli zabezpieczeniowej o poziomie nienaruszalności bezpieczeństwa SIL 2. W pętli zabezpieczeniowej o poziomie nienaruszalności bezpieczeństwa SIL 3 przetwornik powinien być stosowany wraz z przetwornikiem wykorzystującym inną zasadę pomiaru. Dwa przetworniki Promag pracujące w redundancji homogenicznej nie spełniają wymagań dla poziomu nienaruszalności bezpieczeństwa SIL 3.

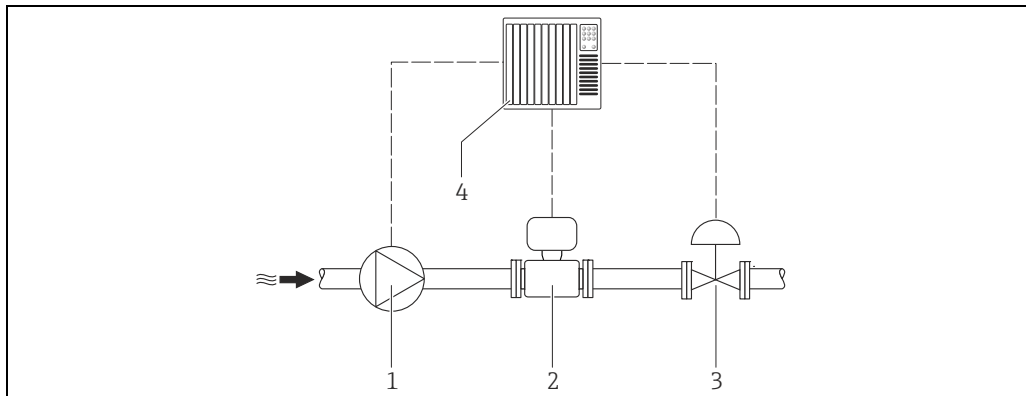


Wskazówka!

Informacje ogólne dotyczące bezpieczeństwa funkcjonalnego (SIL), patrz: www.pl.endress.com/sil i w broszurze dot. kompetencji CP01008Z11 "Bezpieczeństwo funkcjonalne w przemyśle procesowym - zmniejszanie ryzyka przy użyciu przyrządowych systemów bezpieczeństwa" (dostępnym do pobrania ze strony: www.pl.endress.com → Do pobrania → Kod dokumentu: CP01008Z11).

Konfiguracja układu pomiarowego z przetwornikiem Promag 50, 53

Elementy układu pomiarowego



Elementy układu pomiarowego

- 1 Pompa
- 2 Przetwornik pomiarowy
- 3 Zawór
- 4 System automatyki

Przetwornik generuje sygnał analogowy (4...20 mA) proporcjonalny do wartości przepływu. Jest on przesyłany dalej do systemu sterowania, który analizuje go celem ustalenia, czy przekracza on zadaną wartość graniczną w górę lub w dół.



Wskazówka!

- Sygnałem wyjściowym służącym do realizacji funkcji bezpieczeństwa jest sygnał analogowy 4...20 mA. Wszystkie funkcje bezpieczeństwa odnoszą się wyłącznie do wyjścia prądowego 1.
- Przetwornik pomiarowy musi być zabezpieczony przed nieuprawnionym dostępem → patrz rozdział "Blokada zapisu danych konfiguracyjnych" (→ 7).
- Aplikacja systemu bezpieczeństwa została zaprojektowana w taki sposób, aby funkcja bezpieczeństwa zadziałała w przypadku przekroczenia zakresu w górę (fail high) i w dół (fail low) niezależnie od skutków (stan bezpieczny lub niebezpieczny systemu).
- Jeśli komunikacja odbywa się również za pośrednictwem protokołu HART, w przetworniku Promag 53 musi być włączona ochrona zapisu HART → patrz rozdział "Blokada zapisu danych konfiguracyjnych" (→ 7).

Parametry związane z bezpieczeństwem funkcjonalnym (patrz dodatek) dotyczą wyłącznie wyjścia prądowego (4 do 20 mA) w następujących wersji przyrządu:

- Promag 50***_*****(*)
(*) = pozycja kodu zam. "Wyjście, wejście, opcje: A / W / D / S / T
- Promag 53***_*****(*)
(*) = pozycja kodu zam. "Wyjście, wejście, opcje: A / B / C / L / M / S / T / 2 / 4

Parametry funkcji bezpieczeństwa

Informacje na temat niezbędnych ustawień i parametrów funkcji bezpieczeństwa podano w rozdziale "Ustawienia i instrukcje montażu" (→ 6) i w dodatku (→ 15). Czas odpowiedzi układu pomiarowego wynosi ≤ 2 s. Alarm funkcji monitorowania jest aktywowany po upływie czasu odpowiedzi i opóźnienia.



Wskazówka!

Czas przywracania zdadności oprzyrządowania do użycia wynosi 8 godzin (MTTR).

Dokumentacja uzupełniająca

Do układu pomiarowego musi być dołączona następująca dokumentacja:

Typ urządzenia	Instrukcja obsługi	Opis funkcji przyrządu
Promag 50	BA00046D/31	BA00049D/31
Promag 53	BA00047D/31	BA00048D/31

Dokument ten zawiera również informacje na temat dopuszczalnych parametrów pracy i warunków otoczenia, a także parametrów funkcjonalnych wyjścia prądowego.

W przypadku urządzeń w wersji przeciwybuchowej, należy zapoznać się z odpowiednią Instrukcją dot. bezpieczeństwa Ex (XA) lub Schematem montażowym (ZD).

Ustawienia i instrukcje montażu

Instrukcje montażu

Instrukcje poprawnego montażu przetwornika można znaleźć w załączonej Instrukcji obsługi (BA) → patrz "Dokumentacja uzupełniająca" (→ 5).

Możliwość zastosowania przyrządu

Należy starannie dobrać średnicę nominalną czujnika, odpowiednio do natężenia przepływu spodziewanego w danej aplikacji pomiarowej. Maksymalne natężenie przepływu podczas pracy nie może przekroczyć podanej wartości maksymalnej dla czujnika przepływu. W aplikacjach związanych z bezpieczeństwem funkcjonalnym zaleca się również, aby ustawiona dolna wartość graniczna przepływu nie była mniejsza od 5% ustawionej wartości przepływu maksymalnego dla czujnika.

Układ pomiarowy powinien być dostosowany do konkretnej aplikacji, z uwzględnieniem własności medium i warunków otoczenia. Należy ściśle przestrzegać wskazówek dotyczących krytycznych parametrów procesu i warunków montażowych podanych w instrukcji obsługi przyrządu.

Unikać aplikacji, w których może wystąpić zjawisko gromadzenia się osadu, korozji lub erozji rury pomiarowej.

Dla mediów ciekłych, jednofazowych, o własnościach zbliżonych do wody nie ma żadnych specjalnych wymagań.



Wskazówka!

W celu uzyskania dalszych informacji, prosimy o kontakt z biurem Endress+Hauser.

Instrukcje konfiguracji

W systemach sterowania procesem parametryzacja przetwornika może być wykonywana za pomocą:

- elementów obsługowych na wskaźniku (LCD)
- komunikatora ręcznego HART DXR 375
- zdalnie z komputera PC z zainstalowanym oprogramowaniem obsługowym i konfiguracyjnym (np. "FieldCare")

Umożliwiają one również uzyskanie informacji o zainstalowanej wersji oprogramowania. → 5

Dodatkowe informacje dotyczące parametryzacji podano w odpowiednich Instrukcjach obsługi → patrz "Dokumentacja uzupełniająca" ().

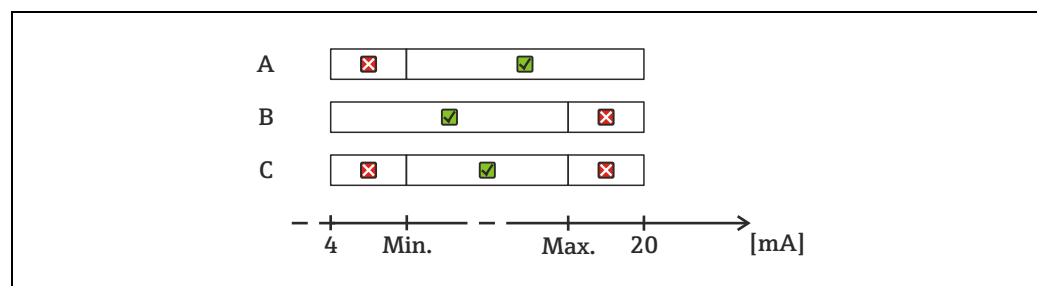
Opcje monitorowania



Przepływomierz może być zastosowany w systemach bezpieczeństwa do monitorowania wartości przepływu objętościowego (minimalnej, maksymalnej i zakresu).

Wskazówka!

Dla zagwarantowania bezpieczeństwa pracy, przepływomierz musi być odpowiednio zamontowany.



A0015277

Opcje monitorowania w systemach bezpieczeństwa

- A Sygnalizacja przekroczenia minimum
- B Sygnalizacja przekroczenia maksimum
- C Monitorowanie zadanego zakresu wartości

- = Aktywacja funkcji bezpieczeństwa
- = Zakres dopuszczalny

Poniższa tabela pokazuje ustawienia niezbędne do stosowania urządzenia pomiarowego w aplikacjach związanych z bezpieczeństwem funkcjonalnym. Ustawienia odnoszą się do wartości na wyjściu prądowym 4...20 mA, proporcjonalnych do wartości przepływu.

Grupa	Nazwa funkcji w grupie	Dopuszczalne ustawienie, gdy przetwornik Promag jest wykorzystywany do realizacji funkcji bezpieczeństwa
WYJŚCIE PRĄDOWE	PRZYPISANIE PRĄDU WYJŚCIOWEGO	Przepływ objętościowy
WYJŚCIE PRĄDOWE	ZAKRES PRĄDOWY	<ul style="list-style-type: none"> - 4-20 mA (.....): Zakres wyjścia prądowego zawsze ustawiony na 4...20 mA. - 0...20 mA: Ustawienie niedozwolone. <p>Promag 50 Niedozwolone są wszystkie opcje konfiguracji 4...20 mA z komunikacją HART.</p> <p>Promag 53 Wszystkie opcje konfiguracji 4...20 mA z komunikacją HART są dozwolone wyłącznie wtedy, gdy aktywna jest ochrona zapisu HART (→ 7, rozdział "Blokada zapisu danych konfiguracyjnych")</p>
WYJŚCIE PRĄDOWE	TRYB BEZPIECZNY	<ul style="list-style-type: none"> - Prąd minimalny - Prąd maksymalny
WYJŚCIE PRĄDOWE	SYMULACJA PRĄDU	WYŁ.
PARAMETRY SYSTEMOWE	ZEROWANIE WSKAZAŃ	WYŁ.
NADZÓR	PRZYPISANIE BŁĘDU SYSTEMOWEGO	WYŁ. (nie można zmieniać przypisania komunikatów informacyjnych i komunikatów dotyczących usterek do innych kategorii)
NADZÓR	OPÓŹNIENIE ALARMU	0...20 s
SYMULACJA SYSTEMU	SYMULACJA TRYBU BEZPIECZNEGO	WYŁ.
SYMULACJA SYSTEMU	SYMULACJA WARTOŚCI MIERZONEJ	WYŁ.

Szczegółowy opis funkcji urządzenia można znaleźć w odpowiedniej dokumentacji "Opis funkcji przyrządu" → patrz "Dokumentacja uzupełniająca" (→ 5).

Blokada zapisu danych konfiguracyjnych

Aby chronić ważne parametry procesu przed zmianą, należy włączyć blokadę programową. Do tego służy kodu użytkownika.

Blokada programowa dla programowania lokalnego	
Funkcja DEFINIOWANIE KODU UŻYTKOWNIKA	Dowolny kod liczbowy (z wyjątkiem 0)

Promag 53:

W przypadku komunikacji HART, ochrona zapisu HART musi być aktywna. Do tego służy zworka na karcie We/Wy. Procedurę aktywacji ochrony zapisu HART podano w odpowiedniej instrukcji obsługi przetwornika → patrz "Dokumentacja uzupełniająca" (→ 5).

Instrukcje konfiguracji jednostki logicznej

Sygnalizator wartości przepływu maks. lub min. (systemu sterowania) należy ustawić na odpowiednią wartość graniczną (w mA, odpowiadającą wartości przepływu maks. lub min.). Procedury regulacji i ustawień podano w odpowiedniej instrukcji obsługi → patrz "Dokumentacja uzupełniająca" (→ 5).

Odpowiedź pomiarowa i reakcja przyrządu na stan błędu



Informacje dotyczące odpowiedzi pomiarowej i reakcji przyrządu na stan błędu opisano w odpowiedniej instrukcji obsługi → patrz "Dokumentacja uzupełniająca" (→ 5).

Wskazówka!

- **Naprawa:** Naprawa przyrządu powinna być wykonywana przez Endress+Hauser. Jeśli naprawa jest wykonywana przez inny podmiot, bezpieczeństwo funkcjonalne przyrządu nie jest gwarantowane.
- **Wyjątek:** Dopuszczalna jest wymiana elementów modułowych urządzenia na oryginalne części zamienne, dokonywana przez wykwalifikowany personel klienta, jeśli został on przeszkolony do tego celu przez firmę Endress+Hauser.
- Usterka produktu Endress+Hauser z certyfikatem SIL, używanego w przyrządowym systemie bezpieczeństwa musi zostać zgłoszona na adres: serwis@pl.endress.com, wraz z podaniem typu przyrządu, numeru seryjnego i opisem usterki. Usterki przyrządu muszą być zgłaszane producentowi. Użytkownik dostarcza producentowi szczegółowy raport z opisem usterki i jej wszystkie możliwe skutki. W opisie tym należy również podać informacje, czy uszkodzenie jest niebezpieczne i czy nie mogło być wykryte bezpośrednio.
- W przypadku awarii urządzenia z atestem SIL produkcji Endress+Hauser, zastosowanego do realizacji funkcji bezpieczeństwa, do zwracanego przyrządu powinna być dołączona "Deklaracja dotycząca skażenia i czyszczenia" wraz z adnotacją "Użyty w przyrządowym systemie bezpieczeństwa do realizacji funkcji bezpieczeństwa".

Informacje na temat użytecznego cyklu życia podzespołów elektrycznych



Podane współczynniki usterkowości podzespołów elektrycznych mają zastosowanie do użytecznego cyklu życia określonego w normie PN-EN 61508-2: rozdział 7.4.7.4 uwaga 3.

Wskazówka!

Zgodnie z uwagą NA4 w normie PN-EN 61508-2, producent i właściciel/operator obiektu powinni podjąć odpowiednie kroki w celu zapewnienia dłuższego czasu eksploatacji przyrządu.

Test kontrolny

Test kontrolny układu pomiarowego



Test kontrolny dyspozycyjności funkcji bezpieczeństwa należy przeprowadzać w odpowiednich odstępach czasu. Operator określa częstotliwość testów, która musi być uwzględniona przy wyznaczaniu prawdopodobieństwa niezadziałania funkcji bezpieczeństwa PFD_{avg} , którą realizuje przepływomierz.

Wskazówka!

W przypadku systemów o architekturze jednokanałowej, wartość średniego prawdopodobieństwa niezadziałania funkcji bezpieczeństwa (PFD_{avg}) zależy od pokrycia diagnostycznego testu kontrolnego (PTC) oraz zakładanego czasu zamierzonego użytkowania wg następującego wzoru:

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

A0015275

Test kontrolny powinien być przeprowadzony w taki sposób, aby pozwalał na sprawdzenie poprawności pracy wszystkich części składowych systemu bezpieczeństwa. Każdy test musi zostać w pełni udokumentowany.

Przed testem funkcji bezpieczeństwa należy najpierw sprawdzić dokładność wartości mierzonej (min., maks., zakresu). Polega on na osiągnięciu wartości bliskich ustawionym wartościom granicznym, powodującym przywołanie funkcji bezpieczeństwa (oraz zadziałanie urządzenia wykonawczego). Aby przeprowadzić test funkcji bezpieczeństwa polegającej na przekroczeniu ustawionego zakresu, wystarczy sprawdzić dokładność wartości zmierzonych.

Dla zapewnienia bezpieczeństwa procesu, podczas testu kontrolnego należy podjąć alternatywne środki ostrożności.

Procedura testu kontrolnego przyrządu może być następująca:

1. Sprawdzenie cyfrowych wartości mierzonych

W zależności od zmiennej mierzonej i dostępnego oprzyrządowania należy przeprowadzić jeden z poniższych testów:

- a. Sekwencja A – Sprawdzanie cyfrowej wartości mierzonej za pomocą stanowiska kalibracyjnego

Przepływ objętościowy

Przepływomierz jest ponownie kalibrowany przy użyciu stanowiska kalibracyjnego akredytowanego zgodnie z ISO/IEC 17025. Można tego dokonać bez demontażu przepływomierza, za pomocą mobilnego stanowiska kalibracyjnego lub po zdemontowaniu przepływomierza, na fabrycznym stanowisku kalibracyjnym. Wielkość odchyłki wartości zmierzonej przepływu o wartości zadanej nie może przekroczyć maksymalnego błędu pomiaru podanego w instrukcji obsługi przepływomierza.



Wskazówka!

W celu uzyskania dalszych informacji na temat standardowych metod kalibracji przepływomierzy w miejscu instalacji, prosimy o kontakt z najbliższym biurem sprzedaży Endress+Hauser.

- b. Sekwencja B – Sprawdzanie cyfrowej wartości mierzonej przy użyciu zainstalowanego licznika

Przepływ objętościowy

Kalibrowane naczynie pomiarowe jest napełniane medium, przy zachowaniu wartości przepływu bliskiej monitorowanej wartości granicznej. Różnica objętości medium w naczyniu pomiarowym przed i po napełnieniu jest porównywana z wartościami ze wskazaniem licznika przepływomierza. Wielkość odchyłki nie może przekroczyć maksymalnego błędu pomiaru podanego w instrukcji obsługi przepływomierza. W celu monitorowania zakresu wartości, test ten należy wykonać oddzielnie dla górnej i dolnej wartości granicznej.

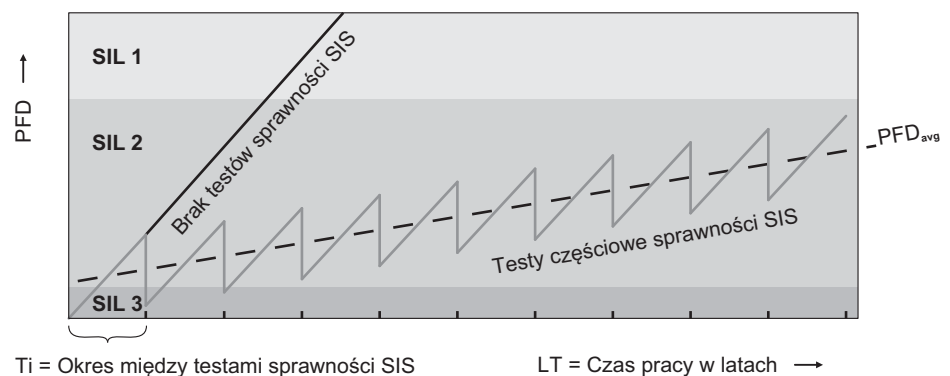
- c. Sekwencja C – Sprawdzanie cyfrowej wartości mierzonej przy użyciu urządzenia Fieldcheck

Przepływ objętościowy

Weryfikacja przepływomierzy za pomocą urządzenia Fieldcheck bez konieczności ich demontażu jest opisana w instrukcji obsługi BA00067D. Fieldcheck automatycznie wyświetla wyniki testu (pozytywny/negatywny).

Ten test można przeprowadzić bez demontażu przepływomierza, co ułatwia przeprowadzanie okresowych przeglądów. Wysokie pokrycie diagnostyczne oznacza, że wykrywanych jest ponad 90 % uszkodzeń niebezpiecznych, dzięki czemu średnie prawdopodobieństwo niezadziałania funkcji bezpieczeństwa PFD_{AVG} jest niższe niż bez wykonania testu (→ rysunek poniżej). Średnie prawdopodobieństwo niezadziałania funkcji bezpieczeństwa PFD_{AVG} można oszacować za pomocą wzoru (→ 9), z uwzględnieniem zakładanego czasu zamierzonego użytkowania t.

Dzięki zastosowaniu oprogramowania "FieldCare" wyniki testów można zaimportować do bazy danych, wydrukować i wykorzystać jako dowód weryfikacji dla właściwego organu certyfikującego.



System o architekturze jednokanałowej 1oo1

A0015615-PL

2. Sprawdzenie wyjścia prądowego 4...20 mA

Użycie opcji symulacji prądu (stała wartość prądu), dostępnej w menu obsługi, powoduje ustawienie sygnałów na wyjściu prądowym przepływomierza: 3.6 mA, 4.0 mA, 20.0 mA i 22.0 mA i porównanie z wynikami pomiaru skalibrowanego, zewnętrznego amperomierza.

3. Sprawdzenie funkcji bezpieczeństwa

Poprawność zadziałania funkcji bezpieczeństwa, w tym urządzenia wykonawczego, musi zostać sprawdzona poprzez ustawienie odpowiednich symulowanych wartości prądu na wyjściu 4...20 mA (nieco poniżej i powyżej punktu przełączania). W celu monitorowania zakresu należy przeprowadzić ten test oddzielnie dla górnej i dolnej wartości granicznej.

4. Zakończenie testu sprawdzającego

Wyłączyć tryb symulacji i przejść do trybu pomiaru wartości mierzonych przepływu.



Wskazówka!

Test sprawdzający uznaje się za wykonany, gdy wykonane zostaną kroki od 1 do 4.

Stosując sekwencje 1A i 1B wykrywanych jest 98% uszkodzeń niebezpiecznych niewykrywalnych, natomiast stosując sekwencję 1C wykrywanych jest 90% uszkodzeń niebezpiecznych niewykrywalnych. Jeśli jedno z kryteriów testów opisanych niżej nie jest spełnione, przyrząd nie może być już wykorzystywany w przyrządowym systemie bezpieczeństwa.

Ten test nie obejmuje wpływu uszkodzeń systematycznych na funkcję bezpieczeństwa, więc wpływ ten musi być oceniany oddzielnie. Uszkodzenia systematyczne mogą być spowodowane np. własnościami medium mierzonego, warunkami pracy, powstawaniem osadu czy korozją.

Streszczenie dla kierownictwa opracowane przez Exida



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

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights on the format of this technical report reserved.



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 B¹ 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 40°C. 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).

Dodatek (parametry związane z bezpieczeństwem funkcjonalnym)

Uwagi wstępne



W zależności od opcji wybranej w kodzie zamówieniowym, przepływomierze Promag są dostarczane z różnymi wersjami modułu wyjść i wejść. Dla zachowania przejrzystości, podobne typy modułów elektroniki pogrupowano w odpowiednie kategorie.

Wskazówka!

- Parametry związane z bezpieczeństwem funkcjonalnym opisano oddzielnie dla każdej z tych kategorii → patrz rozdziały "Kategorie 1-7". Tabele podane w rozdziałach dotyczących tych kategorii zawierają wszystkie ważne parametry charakterystyczne. Ich wartości odnoszą się do wszystkich możliwych zastosowań:
- Podane współczynniki usterkowości uwzględniają wszystkie typy usterek podzespołów elektronicznych wg normy Siemens SN29500 w temperaturze otoczenia +40 °C (+104 °F).

System pomiarowy / moduł elektroniki Kod zamówieniowy	Wyjścia i wejścia	Kategoria → 16
---	-------------------	-------------------

Promag 50

50 *** - *****W	Wyjście prądowe	1
50 *** - *****A	Wyjście prądowe / częstotliwościowe	1
50 *** - *****D	Wyjście prądowe / częstotliwościowe / statusu / wejście statusu	1
50 *** - *****S	Wyjście prądowe aktywne (Ex i) / częstotliwościowe pasywne (Ex i)	6
50 *** - *****T	Wyjście prądowe pasywne (Ex i) / częstotliwościowe pasywne (Ex i)	7

Promag 53

53 *** - *****C	Wyjście prądowe / częstotliwościowe / przekaźnikowe / przekaźnikowe 2	2
53 *** - *****L	Wyjście prądowe / przekaźnikowe / przekaźnikowe 2 / wejście statusu	2
53 *** - *****M	Wyjście prądowe / częstotliwościowe / częstotliwościowe 2 / wejście statusu	2
53*** - *****2	Wyjście prądowe / prądowe 2 / częstotliwościowe / przekaźnikowe	2
53*** - *****4	Wyjście prądowe / częstotliwościowe / przekaźnikowe / wejście prądowe	2
53 *** - *****A	Wyjście prądowe / częstotliwościowe	3
53 *** - *****B	Wyjście prądowe / częstotliwościowe / przekaźnikowe / przekaźnikowe 2	3
53 *** - *****S	Wyjście prądowe aktywne (Ex i) / częstotliwościowe pasywne (Ex i)	4
53 *** - *****T	Wyjście prądowe pasywne (Ex i) / częstotliwościowe pasywne (Ex i)	5

- Opcje dopuszczeń dostępne dla Promag H/P/W: ATEX II2G/D, FM/CSA Cl.1 Div.1, TIIS i NEPSI
- Opcja dopuszczenia dostępna dla Promag E/H/R/W: ATEX II3G/D
- Opcja dopuszczenia dostępna dla Promag D/E/H/R/W: FM/CSA Cl.1 Div.2

Uwagi dotyczące terminu "uszkodzenia niebezpieczne niewykrywalne"

Sytuacje, gdy urządzenie procesowe nie reaguje na przywołanie (np. przepływomierz nie przechodzi do zdefiniowanego wstępnie trybu bezpiecznego) lub gdy odchyłka sygnału wyjściowego jest większa od podanego całkowitego błędu pomiaru. Dodatkowe informacje dotyczące całkowitego błędu pomiaru, podano w rozdziale "Cechy metrologiczne" w instrukcji obsługi konkretnego przepływomierza.

Do analizy FMEDA przyjęto następujące założenia:

- Współczynnik usterkowości jest stały, nie jest uwzględniane zużycie podzespołów.
- Współczynnik wyłączeń zasilania zewnętrznego nie jest uwzględniany.
- Protokół HART wykorzystywany jest wyłącznie do odczytu danych podczas pomiarów.
- Czas przywracania zdatności do użycia wynosi 8 godzin.
- Czas testu reakcji systemu sterowania na wykrytą usterkę wynosi jedną godzinę.
- Wszystkie moduły pracują w trybie "na rzadkie przywołanie".

- W aplikacjach związanych z bezpieczeństwem funkcjonalnym może być wykorzystywane tylko wyjście prądowe 1.
- Nie uwzględniono współczynników usterkowości zewnętrznego źródła zasilania.
- Urządzenie będzie używane w przeciętnych przemysłowych warunkach otoczenia, porównywalnych do klasyfikacji opisanej jako "montaż stacjonarny" w dokumencie MIL-HDBK-217F. Alternatywnie przyjmowane są następujące warunki otoczenia: PN-EN 60654-1, klasa C (miejsca osłonięte), z limitami temperatur odpowiadającymi zaleceniom producenta i średnią temperaturą pracy przetwornika przez dłuższy okres wynoszącą +40 °C (+104 °F). Poziom wilgotności zgodny z zaleceniami producenta.
- Jedynie opisane wersje będą zastosowane w aplikacjach związanych z bezpieczeństwem funkcjonalnym.
- Ponieważ opcjonalny wyświetlacz nie jest elementem realizacji funkcji bezpieczeństwa, w obliczeniach wskaźnik usterkowości wyświetlacza nie jest uwzględniany.
- Aplikacja systemu bezpieczeństwa została zaprojektowana w taki sposób, aby funkcja bezpieczeństwa zadziałała w przypadku przekroczenia zakresu w górę (fail high) i w dół (fail low) niezależnie od skutków (stan bezpieczny lub niebezpieczny systemu).

Kategorie

- SIL (Poziom nienaruszalności bezpieczeństwa) = 2
- Wskaźnik HFT (Tolerancja defektów sprzętu zgodny z rozdziałem 11.4 normy PN-EN 61511-1) = 0
- Typ urządzenia = Typ B (urządzenie złożone)

Kategoria	SFF ¹⁾	PFD _{AVG}			λ_{du}	λ_{dd}	λ_{su}	λ_{sd}
		1 rok	2 lata	5 lat				
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⁾ Udział uszkodzeń bezpiecznych

www.pl.endress.com
