Safety Manual

VEGASWING 61, 63

Двухпроводный (8/16 mA)

с квалификацией SIL

Document ID: 52085

Содержание

Редакция:2016-04-15

52085-RU-160508

1 Язык документации

DE	Das vorliegende *Safety Manual* für Funktionale Sicherheit ist verfügbar in den Sprachen Deutsch, Englisch, Französisch und Russisch.
EN	The current *Safety Manual* for Functional Safety is available in German, English, French and Russian language.
FR	Le présent *Safety Manual* de sécurité fonctionnelle est disponible dans les langues suivantes: allemand, anglais, français et russe.
RU	Данное руководство по функциональной безопасности *Safety Manual* имеется на немецком, английском, французском и русском языках.

52085-RU-160508

2 Сфера действия

2.1 Исполнение устройства

Данное руководство по безопасности действует для сигнализаторов предельного уровня

VEGASWING 61 с квалификацией SIL

VEGASWING 63 с квалификацией SIL

Блок электроники:

- Двухпроводный (8/16 mA)

2.2 Область применения

Датчик может применяться для сигнализации уровня на жидкостях в связанных с безопасностью системах, в соответствии с IEC 61508, в режимах работы *low demand mode* (с низкой частотой запросов) или *high demand mode* (с высокой частотой запросов):

- До SIL2 в одноканальной архитектуре
- До SIL3 в многоканальной архитектуре (систематическая пригодность SC3)

Для выдачи измеренных значений могут использоваться следующие интерфейсы:

- Двухпроводный - токовый выход 8/16 mA

2.3 Соответствие SIL

Соответствие SIL было оценено независимой организацией *exida* Certification S.A. по IEC 61508.[1)]

[1)] Удостоверяющие документы см. в Приложении.

3 Проектирование

3.1 Функция безопасности

Функция безопасности

Для контроля одного предела уровня датчик, через состояния "*вибрирующий элемент не покрыт*" или "*вибрирующий элемент покрыт*", обнаруживает предельный уровень, заданный монтажной позицией датчика.

Обнаруженное состояние сигнализируется на выходе как "*Ток = 8 mA*" или "*Ток = 16 mA*".

3.2 Безопасное состояние

Безопасное состояние

Выбор режима работы производится на устройстве формирования сигнала.

Безопасное состояние, таким образом, зависит от выбранного режима работы.

Режим работы	Защита от переполнения (Режим работы max.)	Защита от сухого хода (Режим работы min.)
Вибрирующий элемент	покрыт	не покрыт
Выходной ток	16 mA, ±1,5 mA	8 mA, ±1,5 mA

Сигналы отказа при нарушении функции

Возможные токи неисправности:

- ≤ 1,8 mA ("fail low")

3.3 Необходимые условия для эксплуатации

Указания и ограничения

- Применение измерительной системы должно соответствовать условиям применения с учетом давления, температуры, плотности и химических свойств среды. Должны выдерживаться границы условий применения.
- Спецификации по данным руководства по эксплуатации, особенно токовая нагрузка выходной цепи, должны выдерживаться в названных пределах.
- При применении как защиты от сухого хода следует предотвращать накопление осадка среды на вибрирующей системе (возможно, что требуются уменьшенные интервалы между проверками (Proof Test Interval)).
- Должны быть приняты во внимание указания в гл. "*Технические показатели безопасности*", п. "*Дополнительные сведения*".
- Все составные части измерительной цепи должны соответствовать предусмотренному уровню полноты безопасности "*Safety Integrity Level (SIL)*".

4 Технические показатели безопасности

4.1 Показатели соотв. IEC 61508

Показатель	Значение
Safety Integrity Level	SIL2 в одноканальной архитектуре SIL3 в многоканальной архитектуре[2)]
Устойчивость к отказам аппаратных средств	HFT = 0
Тип устройства	Typ A
Режим работы	Low demand mode, High demand mode
SFF	> 60 %
MTBF = MTTF + MTTR[3)]	3,13 x 10^6 h (358 лет)
Время реакции на ошибку[4)]	< 1,5 с

Интенсивность отказов

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
7 FIT	0 FIT	35 FIT	35 FIT	141 FIT	0 FIT	8 FIT

PFD_{AVG}	0,030 x 10^{-2}	(T1 = 1 год)
PFD_{AVG}	0,085 x 10^{-2}	(T1 = 5 лет)
PFD_{AVG}	0,154 x 10^{-2}	(T1 = 10 лет)
PFH	0,035 x 10^{-6} 1/ч	

Охват при контрольной проверке (PTC)

Вид проверки[5)]	Остающиеся интенсивности отказов опасных необнаруженных отказов	PTC
Проверка 1	14 FIT	60 %
Проверка 2	2 FIT	96 %

4.2 Показатели соотв. ISO 13849-1

Согласно ISO 13849-1 (безопасность машин), из технических показателей безопасности производятся следующие показатели:[6)]

Показатель	Значение
MTTFd	541 год
DC	83 %
Performance Level	3,50 x 10^{-8} 1/ч (соответствует "e")

2) Возможна однородная избыточность.
3) Включая ошибки, лежащие вне пределов функции безопасности.
4) Время между наступлением события и выдачей сигнала неисправности.
5) См. п. "Контрольная проверка".
6) ISO 13849-1 не был предметом сертификации устройства.

52085-RU-160508

4.3 Дополнительные сведения

Определение интенсивностей отказов

Интенсивности отказов устройства рассчитаны посредством FMEDA по IEC 61508. В основе расчетов лежат интенсивности отказов конструктивных элементов по **SN 29500** со следующими данными.

Все числовые значения относятся к средней температуре окружающей среды во время эксплуатации 40 °C (104 °F). Для более высоких температур значения должны корректироваться:

- Для длительной температуры эксплуатации > 50 °C (122 °F), с коэффициентом 1,3
- Для длительной температуры эксплуатации > 60 °C (140 °F), с коэффициентом 2,5

Аналогичные коэффициенты действительны, если следует ожидать частых колебаний температуры.

Допущения FMEDA

- Интенсивности отказов постоянные. При этом должен учитываться полезный срок службы конструктивных элементов согласно IEC 61508-2.
- Множественные отказы не учитываются.
- Износ механических частей не учитывается.
- Интенсивности отказов внешних источников питания в расчет не включаются.
- Окружающие условия соответствуют средним промышленным условиям.

Расчет PFD_{AVG}

Приведенные выше значения для PFD_{AVG} были рассчитаны для архитектуры 1oo1 следующим образом:

$$PFD_{AVG} = \frac{PTC \times \lambda_{DU} \times T1}{2} + \lambda_{DD} \times MTTR + \frac{(1 - PTC) \times \lambda_{DU} \times LT}{2}$$

Использованные параметры:

- T1 = Proof Test Interval
- PTC = 90 %
- LT = 10 лет
- MTTR = 24 h

Конфигурация блока формирования сигнала

Подключенный блок управления и обработки сигнала должен иметь следующие свойства:

- Сигналы отказа измерительной системы оцениваются по принципу тока покоя.
- Сигналы "*fail low*" и "*fail high*"интерпретируются как неисправность, вследствие чего должно приниматься безопасное состояние!

В ином случае, соответствующие доли интенсивностей отказов должны быть присвоены опасным отказам и произведен новый расчет значений, указанных в гл. "*Технические показатели безопасности*"!

Многоканальная архитектура

На основании систематической пригодности SC3, данное устройство может использоваться также с однородным

резервированием в многоканальных системах до уровня полноты безопасности SIL3.

Расчет технических показателей безопасности должен производиться специально для выбранной структуры измерительной цепи на основании указанных интенсивностей отказов. При этом должен учитываться применимый фактор общей причины (common cause factor, CCF) (см. IEC 61508-6, Приложение D).

5 Пуск в эксплуатацию

5.1 Общее

Монтаж и установка

Требуется выполнять содержащиеся в руководстве по эксплуатации рекомендации по монтажу и подключению.

Пуск в эксплуатацию должен выполняться при условиях процесса.

5.2 Указания по настройке

Элементы настройки

Настроечные элементы должны быть установлены в соответствии с предусмотренной функцией безопасности:

- Режим работы (min./max.) устанавливается на устройстве формирования сигнала.
- Ползунковый переключатель для переключения чувствительности

Функции элементов настройки описаны в руководстве по эксплуатации.

Следует принять во внимание!

SIL Во время выполнения установок функция безопасности должна рассматриваться как ненадежная!

При необходимости, должны предприниматься другие меры для поддержания функции безопасности.

SIL В отношении задержки включения/выключения должна соблюдаться согласованность суммы всех задержек переключения от датчика до исполнительного элемента с временем безопасности процесса!

SIL Устройство должно быть защищено от случайной или несанкционированной настройки!

6 Диагностика и сервис

6.1 Поведение при отказе

Внутренняя диагностика

Устройство постоянно контролируется внутренней диагностической системой. При обнаружении функционального сбоя, соответствующие выходные сигналы принимают безопасное состояние (см. разд. "*Безопасное состояние*").

Время реакции на ошибку дано в гл. "*Технические показатели безопасности*".

SIL

При установленных отказах вся измерительная система должна быть выведена из работы, а безопасное состояние процесса должно поддерживаться другими мерами.

О появлении опасного необнаруженного отказа следует сообщить производителю (с приложением описания ошибки).

6.2 Ремонт

Замена электроники

Соответствующая процедура описана в руководстве по эксплуатации. Следует соблюдать указания по начальной установке.

52085-RU-160508

7 Контрольная проверка

7.1 Общее

Постановка цели

Для обнаружения возможных опасных необнаруженных отказов, функция безопасности должна проверяться через соответствующие промежутки времени посредством контрольной проверки. Выбор вида проверки является ответственностью лица, эксплуатирующего устройство. Временные интервалы между проверками выбираются, руководствуясь требуемой средней вероятностью опасных ошибок по запросу PFD_{AVG} (см. гл. "*Технические показатели безопасности*").

Для документирования этой проверки может использоваться форма протокола проверки, показанная в Приложении.

Если одна из проверок протекает отрицательно, то вся измерительная система должна быть выведена из работы, а безопасное состояние процесса должно поддерживаться другими мерами.

При многоканальной архитектуре это должно выполняться отдельно для каждого канала.

Подготовка

- Установить функцию безопасности (режим работы, точки переключения)
- При необходимости, устройство удалить из безопасной цепи и поддерживать функцию безопасности иными средствами

Небезопасное состояние устройства

Внимание!
Во время функционального теста функция безопасности должна рассматриваться как небезопасная. Следует учитывать, что функциональный тест оказывает влияние на подключенные устройства.

При необходимости, должны предприниматься другие меры для поддержания функции безопасности.

После завершения функционального теста должно быть восстановлено состояние, определенное для функции безопасности.

7.2 Проверка 1 - без заполнения/опорожнения или демонтажа датчика

Условия

- Устройство может оставаться в смонтированном состоянии.
- Выходной сигнал соответствует уровню (покрытый или непокрытый вибрирующий элемент).

Процедура

1. Выполнить перезапуск (нажать тестовую кнопку на устройстве формирования сигнала или выключить и снова включить устройство).
2. Оценить моделируемые рабочие состояния при запуске.

Ожидаемый результат

Устройство выдает определенный пусковой ток в три стадии:

Сигнал неисправности – Сигнал "пусто" – Сигнал "полно" (см. Руководство по эксплуатации). После этого, выходной сигнал соответствует уровню заполнения.

Охват проверки

См. *Технические показатели безопасности*

7.3 Проверка 2 - с заполнением/ опорожнением или демонтажом датчика

Условия

- **Альтернатива 1:** устройство остается в смонтированном состоянии и есть возможность вызвать смену состояний "*вибрирующий элемент не покрыт*"/"*вибрирующий элемент покрыт*" посредством заполнения или опорожнения емкости.
- **Альтернатива 2:** устройство демонтировано и есть возможность вызвать смену состояний "*вибрирующий элемент не покрыт*"/"*вибрирующий элемент покрыт*" опусканием в исходный продукт.
- Выходной сигнал соответствует уровню (покрытый или непокрытый вибрирующий элемент).

Процедура

Выполнить заполнение или опорожнение до точки переключения или погрузить датчик в оригинальный заполняющий продукт и оценить соответствующее состояние переключения путем измерения тока.

Ожидаемый результат

Токовое значение выходного сигнала соответствует измененному уровню заполнения (16 mA ±1,5 mA или 8 mA ±1,5 mA)

Охват проверки

См. *Технические показатели безопасности*

8 Приложение A - Протокол проверки

Идентификация	
Фирма/Проверяющее лицо	
ТЕГ установки/устройства	
ТЕГ места измерения	
Тип устройства/Код заказа	
Серийный номер устройства	
Дата начальной установки	
Дата последней проверки функции	

Основание проверки		**Объем проверки**	
(…)	Начальная установка	(…)	Без заполнения емкости или демонтажа датчика
(…)	Контрольная проверка	(…)	С заполнением емкости или демонтажом датчика

Режим работы		**Чувствительность**	
(…)	Защита от переполнения	(…)	≥ 0,7 г/см³ (0.025 lbs/in³)
(…)	Защита от сухого хода	(…)	≥ 0,5 г/см³ (0.018 lbs/in³)

Результат проверки

Шаг проверки	**Уровень**	**Ожидаемое измеренное значение**	**Действительное значение**	**Результат проверки**

Подтверждение	
Дата:	Подпись:

9 Приложение B - Определения понятий

Аббревиатуры

SIL	Safety Integrity Level (SIL1, SIL2, SIL3, SIL4)
SC	Systematic Capability (SC1, SC2, SC3, SC4)
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{AVG}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of a dangerous failure per hour (Ed.2)
FMEDA	Failure Mode, Effects and Diagnostics Analysis
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
λ_S	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_H	Rate for failure, who causes a high output current (> 21 mA)
λ_L	Rate for failure, who causes a low output current (≤ 3.6 mA)
λ_{AD}	Rate for diagnostic failure (detected)
λ_{AU}	Rate for diagnostic failure (undetected)
DC	Diagnostic Coverage
PTC	Proof Test Coverage
T1	Proof Test Interval
LT	Useful Life Time
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration (Ed.2)
MRT	Mean Repair Time
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

52085-RU-160508

10 Приложение C - Соответствие SIL

SIL Declaration of conformity

Functional safety according to IEC 61508 / IEC 61511 / NE130

Vibrating level switch

VEGASWING 61, 63

Two-wire

VEGA Grieshaber KG hereby declares, in sole responsibility, that the instruments can be used for level detection of liquids in a safety-related system according to IEC 61508:

- Up to SIL2 / HFT=0 in a single-channel architecture
- Up to SIL3 / HFT=1 in a multiple-channel architecture

Level of Integrity to:

- Systematic Capability: SC3 (SIL3 capable)
- Random Capability: Type A Element

Safety-related characteristics [1)]

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	SFF	PFD_{AVG} [2)]	PTC1	PTC2
7 FIT	0 FIT	35 FIT	35 FIT	141 FIT	84%	$0{,}030 \times 10^{-2}$	60%	96%

[1)] independently evaluated by exida as per IEC 61508-2:2010

[2)] calculated with T1= 1 year and PTC=90%

This declaration of conformity applies only in connection with the valid operating and safety instructions manuals from VEGA.

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany

07.03.2016

i.V. Thomas Deck
Entwicklung / R&D

SIL_VEGASWING 61, 63 (Z)

52085-RU-160508

Failure Modes, Effects and Diagnostic Analysis

Project:
VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex)
Level limit switch with two-wire output 8mA / 16mA
Applications with level limit detection in liquids (MIN / MAX detection)

Customer:
VEGA Grieshaber KG
Schiltach
Germany

Contract No.:VEGA 03/4-04
Report No.: VEGA 03/4-04 R002
Version V2, Revision R1; August 7, 2015
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex). The devices manufactured in the USA by the Ohmart / VEGA Corporation carry the same name and are identically constructed under comparable quality aspects. Table 1 gives an overview of the different configurations that exist.

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) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Overview of the considered variants

VEGASWING 61	Standard (fixed length)
VEGASWING 63	Tube version (variable length)

The different devices can be equipped with:

- Fork-variants uncoated, coated, enamels
- High temperature version with temperature separator

For safety applications only the described variants of the VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex) have been considered. All other possible variants and configurations are not covered by this report.

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N3]). This failure rate database is specified in the safety requirements specification from VEGA Grieshaber KG for the VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex).

The VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex) can be considered to be Type A[1] elements with a hardware fault tolerance of 0.

For Type A components with a SFF of 60% to < 90% a hardware fault tolerance of 0 according to table 2 of IEC 61508-2 is sufficient for SIL 2 (sub-) systems.

The qualitative analysis of the forks (see [D14]) has shown that only unspecified use of the forks or incorrect installation can lead to an unintended system reaction. All other faults lead to a safe state. Therefore a failure rate of the fork is not included in the calculation. However, the failure rates of all other parts of the sensor system have been considered.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on whether the VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex).are working as "high level switches" or "low level switches". For these applications the following tables show how the above stated requirements are fulfilled.

[1] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

Table 2: VEGASWING 6* Z (MIN detection) – failure rates per IEC 61508:2010

Failure category	SN29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**7**
Fail Dangerous Detected (λ_{DD})	**176**
Fail Dangerous Detected (λ_{dd}), detected by internal diagnostics	0
Fail Annunciation Detected (λ_{AD}) , detected by internal diagnostics	0
Fail High (λ_{H}), detected by safety logic solver	35
Fail Low (λ_{L}), detected by safety logic solver)	141
Fail Dangerous Undetected (λ_{DU})	**35**
Fail Annunciation Undetected (λ_{AU})	8
No effect	76
No part	17
Total failure rate of the safety function (λ_{Total})	**218**
Safe failure fraction (SFF) [2]	**84%**
DC_D	**83%**
SIL AC [3]	**SIL 2**

[2] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.
[3] SIL AC (architectural constraints) will need to be evaluated on sensor subsystem level. The indicated value if is for reference only and means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

Table 3: VEGASWING 6* Z (MAX detection) – failure rates per IEC 61508:2010

Failure category	SN29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**17**
Fail Dangerous Detected (λ_{DD})	**176**
Fail Dangerous Detected (λ_{dd}), detected by internal diagnostics	0
Fail Annunciation Detected (λ_{AD}) , detected by internal diagnostics	0
Fail High (λ_{H}), detected by safety logic solver	35
Fail Low (λ_{L}), detected by safety logic solver)	141
Fail Dangerous Undetected (λ_{DU})	**25**
Fail Annunciation Undetected (λ_{AU})	8
No effect	76
No part	17
Total failure rate of the safety function (λ_{Total})	**218**
Safe failure fraction (SFF) [6]	**88%**
DC_D	**87%**
SIL AC [7]	**SIL 2**

The failure rates are valid for the useful life of the VEGASWING 61 / 63 with oscillator SWING E60 Z (Ex) (see Appendix A) when operating as defined in the considered scenarios.

[6] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.
[7] SIL AC (architectural constraints) will need to be evaluated on sensor subsystem level. The indicated value if is for reference only and means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

Дата печати:

Вся приведенная здесь информация о комплектности поставки, применении и условиях эксплуатации датчиков и систем обработки сигнала соответствует фактическим данным на момент.
Возможны изменения технических данных

52085-RU-160508

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany

Phone +49 7836 50-0
Fax +49 7836 50-201
E-mail: info.de@vega.com
www.vega.com