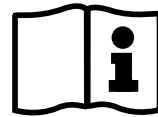


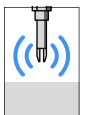
Safety Manual

VEGASWING серии 60

- NAMUR



Document ID:
32000



Содержание

1	Функциональная безопасность	
1.1	Общие положения	3
1.2	Проектирование	5
1.3	Указания по настройке	7
1.4	Начальная установка	7
1.5	Рабочее состояние и состояние отказа	8
1.6	Периодическая функциональная проверка	8
1.7	Показатели техники безопасности	9
2	Приложение	

1 Функциональная безопасность

1.1 Общие положения

Сфера действия

Данное руководство действует для измерительных систем с вибрационными сигнализаторами предельного уровня VEGASWING серии 60 со встроенным блоком электроники SWE60N:

VEGASWING 61, 63



Для устройств с эмалированной вилкой требуется блок электроники SWE60N.E или SWE60N.E1.

Область применения

Данная измерительная система применима для сигнализации предельного уровня жидкостей при особых требованиях безопасности.

В одноканальной архитектуре (1oo1D) обеспечивается уровень совокупной безопасности до SIL2, а в многоканальной избыточной архитектуре - до SIL3.

Соответствие SIL

Соответствие SIL подтверждается документами в Приложении.

Аббревиатуры и термины

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD _{avg}	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
λ_{sd}	Rate for safe detected failure
λ_{su}	Rate for safe undetected failure
λ_{dd}	Rate for dangerous detected failure
λ_{du}	Rate for dangerous undetected failure
DC _S	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd} + \lambda_{su})$
DC _D	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd} + \lambda_{du})$
FIT	Failure In Time (1 FIT = 1 failure/10 ⁹ h)
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair

Аббревиатуры и термины соответствуют определениям по IEC 61508-4.

Применимые нормы

- IEC 61508
 - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511-1
 - Functional safety - safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

Требования безопасности

Предельные значения отказов, в зависимости от класса SIL (IEC 61508-1, 7.6.2)

Уровень безопасности	Режим работы с низкой частотой запросов	Режим работы с высокой частотой запросов
SIL	PFD _{avg}	PFH
4	$\geq 10^{-5} \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-4} \dots < 10^{-3}$	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-3} \dots < 10^{-2}$	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$

Безопасность аппаратных средств для подсистем безопасности типа A (IEC 61508-2, 7.4.3)

Доля безопасных отказов	Отказоустойчивость аппаратных средств			
	SFF	HFT = 0	HFT = 1	HFT = 2
< 60 %		SIL1	SIL2	SIL3
60 % ... < 90 %		SIL2	SIL3	(SIL4)
90 % ... < 99 %		SIL3	(SIL4)	(SIL4)
≥ 99 %		SIL3	(SIL4)	(SIL4)

Эксплуатационная надежность

В соответствии с IEC 61511-1, п. 11.4.4 аппаратная отказоустойчивость HFT для эксплуатационно надежной системы может быть уменьшена на один при следующих условиях:

- Устройство эксплуатационно надежно
- На устройстве могут быть изменены только релеватные для процесса параметры (например: диапазон измерения, токовый выход в состоянии отказа ...)

- Изменение этих релевантных для процесса параметров защищено (например, паролем ...)
- Функция безопасности требует уровня менее SIL4

Оценка способов изменения была включена в подтверждение эксплуатационной надежности.

1.2 Проектирование

Функция безопасности

Функция безопасности данной измерительной системы состоит в регистрации и сигнализации состояния вибрирующего элемента.

Различаются два состояния "покрыт" и "не покрыт".

Безопасное состояние

Безопасное состояние зависит от режима работы:

	Защита от переполнения (режим Max)	Защита от сухого хода (режим Min)
Вибрирующий элемент в безопасном состоянии	покрыт	не покрыт
Выходной ток в безопасном состоянии	0,4 ... 1 mA	0,4 ... 1 mA
Токовый сигнал неисправности "fail low"	< 1 mA	< 1 mA
Токовый сигнал неисправности "fail high"	> 6,5 mA	> 6,5 mA

Описание ошибок

Безопасный отказ имеет место, когда измерительная система без запроса процесса переходит в заданное безопасное состояние или состояние отказа.

Опасный необнаруженный отказ (dangerous undetected failure) имеет место, если измерительная система не переходит в заданное безопасное состояние при запросе процесса.

Конфигурация блока формирования сигнала

Если измерительная система выдает выходной токовый сигнал "fail low" или "fail high", то это должно происходить из-за имеющей место неисправности.

Устройство формирования сигнала поэтому должно интерпретировать такие токовые значения как неисправность и выдавать соответствующий сигнал.

Если этого не происходит, то соответствующие части степеней отказов должны быть присвоены опасным отказам. Тем самым могут быть ухудшены числовые значения в гл. "Числовые показатели техники безопасности".

Блок формирования сигнала должен соответствовать уровню SIL измерительной цепи.

Режим работы на разделительном усилителе NAMUR согласно IEC 60947-5-6 должен быть установлен так, чтобы его переключающий выход при входном токе $< 1,2 \text{ mA}$ принимал безопасное состояние.

Режим работы с низкой частотой запросов

Если частота запросов составляет не более одного раза в год, то измерительная система как часть системы безопасности должна быть установлена в режиме "низкой частоты запросов" ("*low demand mode*") по IEC 61508-4, 3.5.12).

Если отношение частоты диагностических проверок самой измерительной системы к частоте запросов превышает 100, то эту измерительную систему можно рассматривать как исполняющую функцию безопасности в режиме работы с низкой частотой запросов (IEC 61508-2, 7.4.3.2.5).

Соответствующим параметром является значение PFD_{avg} (средняя вероятность опасной ошибки при запросе). Это значение зависит от интервала T_{Proof} между функциональными проверками защитной функции.

Числовые значения см. в п. "*Показатели техники безопасности*".

Режим работы с высокой частотой запросов

Если "*Режим работы с низкой частотой запросов*" не соответствует имеющимся условиям, то измерительная система как часть системы безопасности должна быть установлена в режиме "высокой частоты запросов" ("*high demand mode*") по IEC 61508-4, 3.5.12).

Время отказоустойчивости всей системы при этом должно быть больше суммарного времени реакции или суммы сроков диагностических проверок всех компонентов измерительной цепи.

Соответствующим параметром является значение PFH (частота отказов).

Числовые значения см. в п. "*Показатели техники безопасности*".

Допущения

При выполнении FMEDA были учтены следующие основные условия:

- Частота отказов является постоянной, механический износ деталей не рассматривается
- Частота отказов из-за внешнего источника питания не включается в расчет
- Многократные ошибки не рассматриваются
- Средняя температура окружающей среды во время работы составляет $40 \text{ }^{\circ}\text{C}$ ($104 \text{ }^{\circ}\text{F}$)
- Окружающие условия соответствуют средним промышленным условиям

- Срок службы деталей составляет от 8 до 12 лет (IEC 61508-2, 7.4.7.4, примечание 3)
- Время ремонта (замены измерительной системы) после безопасного отказа составляет восемь (MTTR = 8 h)
- Устройство формирования сигнала может интерпретировать отказы "fail low" и "fail high" как неисправности и выдавать соответствующие сигналы
- Чтобы реагировать на опасные обнаруживаемые отказы, интервал опроса подключенного устройства управления и формирования сигнала составляет макс. 1 час

Общие указания и ограничения

Измерительная система должна устанавливаться соответственно применению с учетом давления, температуры, плотности и химических свойств среды.

Соблюдаются специфические для данного применения предельные значения. Не разрешается выходить за пределы спецификаций, содержащихся в руководстве по эксплуатации.

При применении для защиты от сухого хода должно соблюдаться следующее:

- Предотвращать налипание продукта на вибрирующую систему (возможно, потребуются более короткие интервалы между контрольными проверками)
- Предотвращать присутствие в продукте твердых тел > 5 мм (0.2 in)
- Предотвращать образование пены с плотностью > 0,5 г/см³ (0.018 фунт/дюйм³)

1.3 Указания по настройке

Элементы настройки

Поскольку условия монтажа оказывают влияние на функциональную безопасность измерительной системы, элементы настройки должны быть установлены в соответствии с применением.

- DIL-переключатель для обращения характеристики
- DIL-переключатель установки чувствительности

Функции элементов настройки описаны в руководстве по эксплуатации.

1.4 Начальная установка

Монтаж и установка

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

При пуске в эксплуатацию рекомендуется посредством первого заполнения проверить функцию безопасности.

1.5 Рабочее состояние и состояние отказа

Работа и неисправность

Во время эксплуатации не разрешается изменять установочные элементы и установленные параметры.

При изменениях во время работы должна соблюдаться функция безопасности.

Возможные сообщения об ошибках описаны в руководстве по эксплуатации.

При обнаружении ошибок или сообщениях об ошибках работа всей измерительной системы должна быть остановлена, а безопасность процесса должна поддерживаться другими мерами.

Порядок замены электроники прост и описан в руководстве по эксплуатации. При этом следует соблюдать указания по параметрированию и начальной установке.

Если из-за обнаруженной ошибки необходима замена электроники или всего датчика, об этом нужно сообщить изготовителю (вместе с описанием ошибки).

1.6 Периодическая функциональная проверка

Обоснование

Периодическая проверка служит для проверки функции безопасности и выявления необнаруживаемых опасных ошибок. Работоспособность измерительной системы должна проверяться через определенные промежутки времени. Ответственность за выбор вида проверки лежит на лице, эксплуатирующем оборудование. Временные интервалы между проверками устанавливаются с учетом значения PFD_{avg} в соответствии с таблицей и диаграммой в п. "Показатели техники безопасности"

При высокой частоте запросов, согласно IEC 61508, периодическая функциональная проверка не предусматривается. Доказательством работоспособности измерительной системы является частое обращение к ней. Однако при двухканальной архитектуре для подтверждения избыточного действия есть смысл проводить периодическую функциональную проверку через определенные промежутки времени.

Выполнение

Проверку следует выполнять так, чтобы она подтверждала функцию безопасности во взаимодействии всех компонентов. Это можно обеспечить путем достижения порога срабатывания при заполнении емкости. Если заполнение емкости до уровня срабатывания не является удобным, то срабатывание измерительной системы можно вызвать путем моделирования уровня или физического измерительного эффекта.

Должна быть описана методика проверки и охарактеризована пригодность применяемых методов и способов. Сама проверка должна быть задокументирована.

При отрицательном результате проверки работа всей измерительной системы должна быть остановлена, а безопасность процесса должна поддерживаться другими мерами.

При двухканальной архитектуре (1oo2D) данные указания должны выполняться отдельно для каждого канала.

Функциональная проверка подключенных устройств

В режимах работы „max.“ и „min.“ можно посредством **"Клавиши моделирования"** контролировать работоспособность подключенных устройств. Порядок такой проверки подробно описан в руководстве по эксплуатации.



При такой проверке нужно учитывать состояние вибрирующего элемента:

- Режим работы "max.": вибрирующий элемент "не покрыт"
- Режим работы "min.": вибрирующий элемент "покрыт"

1.7 Показатели техники безопасности

Основания

Значения частоты отказов электроники, механических частей датчика и присоединения определены посредством FMEDA в соответствии с IEC 61508. Расчет основан на значениях частоты отказов конструктивных элементов по SN 29500. Все числовые значения даны относительно средней температуры окружающей среды 40 °C (104 °F).

Для более высокой средней температуры 60 °C (140 °F) значения частоты отказов должны умножаться на эмпирический коэффициент 2,5. Аналогичный коэффициент действует при вероятности частых температурных колебаний.

Расчеты основываются на рекомендациях, изложенных в гл. "Проектирование".

Срок пользования

Через 8 - 12 лет значения частоты отказов электронных элементов увеличиваются, из-за чего ухудшаются производные от них значения PFD и PFH (IEC 61508-2, 7.4.7.4, Примечание 3).

Частота отказов

	Защита от переполнения (режим Max/A)	Защита от сухого хода (режим Min/B)
λ_{sd}	9 FIT	9 FIT
λ_{su}	203 FIT	202 FIT

	Защита от переполнения (режим Max/A)	Защита от сухого хода (режим Min/B)
λ_{dd}	9 FIT	9 FIT
λ_{du}	43 FIT	45 FIT
MTBF = MTTF + MTTR	$3,79 \times 10^6$ час	$3,79 \times 10^6$ час

Время реакции на ошибку

Время реакции на ошибку	< 1,5 сек.
-------------------------	------------

Одноканальная архитектура (1oo1D)

Специфические числа

SIL	SIL2
HFT	0
Тип устройства	Тип А

	Защита от переполнения (режим Max/A)	Защита от сухого хода (режим Min/B)
SFF	83 %	83 %
PFD_{avg} T _{Proof} = 1 год T _{Proof} = 5 лет T _{Proof} = 10 лет	< $0,019 \times 10^{-2}$ < $0,095 \times 10^{-2}$ < $0,189 \times 10^{-2}$	< $0,020 \times 10^{-2}$ < $0,097 \times 10^{-2}$ < $0,195 \times 10^{-2}$
PFH	< $0,043 \times 10^{-6}$ /час	< $0,045 \times 10^{-6}$ /час

Временная зависимость PFD_{avg}

В пределах 10 лет зависимость PFD_{avg} от времени работы приближается к линейной. Данные выше значения действительны для временного интервала T_{Proof}, по истечении которого должна проводиться периодическая функциональная проверка.

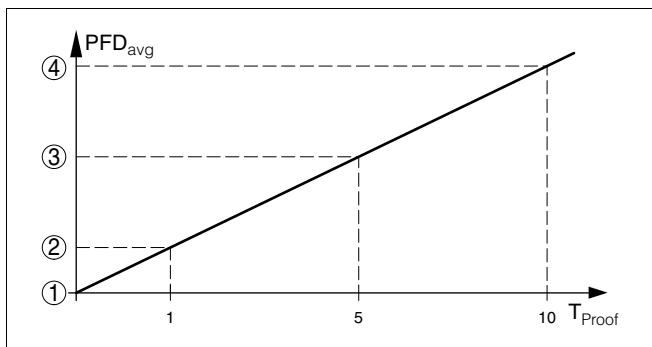


Рис. 1: Изменение PFD_{avg} во времени (числовые значения см. в таблицах выше)

- 1 $PFD_{avg} = 0$
- 2 PFD_{avg} через 1 год
- 3 PFD_{avg} через 5 лет
- 4 PFD_{avg} через 10 лет

Многоканальная архитектура

Специфические числа

При установке измерительной системы в многоканальной архитектуре числовые значения безопасности выбранной структуры измерительной цепи рассчитываются посредством приведенных выше значений частоты отказов специально для выбранного применения.

Необходимо учитывать соответствующий фактор общей причины отказов.

2 Приложение



FMEDA and Proven-in-use Assessment

Project:
VEGASWING 61 / 63 with oscillator SWING E60 N (Ex)
Level limit switch with two-wire NAMUR output
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 R003
Version V1, Revision R1.2, August 2003
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 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 level limit switches VEGASWING 61 / 63 with oscillator SWING E60 N (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) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview

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

The failure rates used in this analysis are based on 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 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.

VEGASWING 61 / 63 with oscillator SWING E60 N (Ex) are considered to be Type A¹ components having 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.

As the level limit switches VEGASWING 61 / 63 with oscillator SWING E60 N (Ex) are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration of the devices was carried out. According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.1 the devices are suitable to be used, as a single device, for SIL 2 safety functions

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.

Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

© exida.com GmbH
Stephan Aschenbrenner

vega 03-4-04 r003 v1 r1.2 August 27, 2003



Table 2: Summary for VEGASWING 6* N (MIN detection)

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD _{AVG} = 1.95E-04	PFD _{AVG} = 9.74E-04	PFD _{AVG} = 1.95E-03	> 83 %

$$\lambda_{sd} = 9,24E-09 \text{ 1/h} = 9 \text{ FIT}$$

$$\lambda_{su} = 2,02E-07 \text{ 1/h} = 202 \text{ FIT}$$

$$\lambda_{dd} = 9,15E-09 \text{ 1/h} = 9 \text{ FIT}$$

$$\lambda_{du} = 4,45E-08 \text{ 1/h} = 45 \text{ FIT}$$

Table 3: Summary for VEGASWING 6* N (MAX detection)

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD _{AVG} = 1.90E-04	PFD _{AVG} = 9.47E-04	PFD _{AVG} = 1.89E-03	> 83 %

$$\lambda_{sd} = 8,74E-09 \text{ 1/h} = 9 \text{ FIT}$$

$$\lambda_{su} = 2,03E-07 \text{ 1/h} = 203 \text{ FIT}$$

$$\lambda_{dd} = 9,15E-09 \text{ 1/h} = 9 \text{ FIT}$$

$$\lambda_{du} = 4,33E-08 \text{ 1/h} = 43 \text{ FIT}$$

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 table 3.1 of ANSI/ISA-84.01-1996 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 functional assessment has shown that the level limit switches VEGASWING 61 / 63 with oscillator SWING E60 N (Ex) have a PFD_{AVG} of 1,95E-04 for MIN detection and a PFD_{AVG} of 1,90E-04 for MAX detection for a proof time period of 1 year and a Safe Failure Fraction (SFF) of > 83%. Based on the verification of "prior use" they can be used as single devices for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the level limit switches VEGASWING 61 / 63 with oscillator SWING E60 N (Ex) 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 for different operating conditions is presented in section 5.3 and 5.4 along with all assumptions.



Дата печати:

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany
Phone +49 78936 50-0
Fax +49 78936 50-201
E-mail: info@de.vega.com
www.vega.com



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

© VEGA Grieshaber KG, Schiltach/Germany 2010