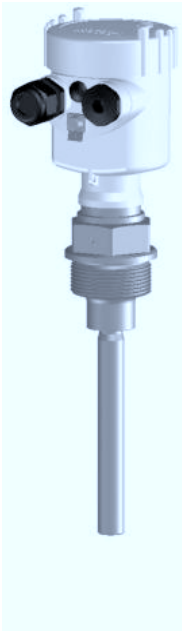
Safety Manual

VEGAVIB серии 60

- NAMUR



Document ID:
32005

Содержание

32005-RU-110531

1 Функциональная безопасность

1.1 Общее

Сфера действия

Данное руководство действует для измерительных систем с вибрационными сигнализаторами предельного уровня VEGAVIB серии 60 со встроенным блоком электроники VB60N:

VEGAVIB 61, 62, 63, 65, 66, 67

Действительные версии аппаратного и программного обеспечения:

- Серийный номер электроники > 14642206
- Программное обеспечение датчика, версия 1.00 и выше

Область применения

Данная измерительная система применима для сигнализации предельного уровня порошкообразных или гранулированных сыпучих продуктов при особых требованиях безопасности, например:

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

Примечание:
Со специальной заводской настройкой измерительная система может также применяться для обнаружения твердых веществ в воде (см. "*Руководство по эксплуатации*").

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 (или DIN EN)
  - Functional safety of electrical/electronic/programmable electronic safety-related systems

Требования безопасности

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

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

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

Доля безопасных отказов			

Отказоустойчивость аппаратных средств
SFF
HFT = 0
HFT = 1
HFT = 2
< 60 %
не разрешено
SIL1
SIL2
60 % … < 90 %
SIL1
SIL2
SIL3
90 % … < 99 %
SIL2

SIL3
(SIL4)
≥ 99 %
SIL3
(SIL4)
(SIL4)

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 определенное безопасное состояние или состояние отказа.

Если внутренняя система диагностики определяет ошибку, измерительная система переходит в состояние отказа.

Опасный необнаруженный отказ (dangerous undetected failure) имеет место, если измерительная система не переходит в определенное 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 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

32005-RU-110531

- Частота отказов из-за внешнего источника питания не включается в расчет
- Многократные ошибки не рассматриваются
- Средняя температура окружающей среды во время работы составляет 40 °C (104 °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 часов (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
- Имеющие коммуникационные интерфейсы (например: HART, I^2C) не используются для передачи релевантных для безопасности данных

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 провекрами)
- Исполнение с вилкой: предотвращать размер частиц продукта > 15 мм (0.6 in)

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.

- Потенциометр для настройки точки переключения
- DIL-переключатель режимов работы

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.

Применяемые методы и способы проверки должны быть указаны и охарактеризованы по степени пригодности. 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 в режиме работы "Защита от переполнения"

Функцональность измерительной системы, используемой для защиты от переполнения, подтверждается простой функциональной проверкой, которая может выполняться и контролироваться вручную или посредством подключенной системы управления.

Данная функциональная проверка проводится путем размыкания кабеля питания не менее чем на две секунды, после чего запуск токового выхода происходит в специальном режиме, который нужно запротоколировать.

Порядое проверки подробно описан в руководстве по эксплуатации.

Кнопка моделирования:

Нажатием кнопки моделирования моделируется размыкание кабеля между датчиком и блоком формирования сигнала.

Примечание:
Данная проверка может выполняться только при непокрытом вибрирующем элементе.

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.

Примечание:
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)	**Защита от сухого хода (режим Min)**
λ_{sd}	12 FIT	36 FIT
λ_{su}	160 FIT	155 FIT
λ_{dd}	390 FIT	366 FIT
λ_{du}	47 FIT	52 FIT
DC_S	7 %	19 %
DC_D	89 %	88 %
MTBF = MTTF + MTTR	1,56 x 10^6 час	1,56 x 10^6 час

Время реакции на ошибку

Длительность диагностической проверки	< 100 сек.

Специфические числа

Одноканальная архитектура (1oo1D)

SIL	SIL2
HFT	0
Тип устройства	Тип B

32005-RU-110531

	Защита от переполнения (режим Max)	Защита от сухого хода (режим Min)
SFF	92 %	91 %
PFD_{avg} T_{Proof} = 1 год T_{Proof} = 5 лет T_{Proof} = 10 лет	< 0,021 x 10^{-2} < 0,104 x 10^{-2} < 0,207 x 10^{-2}	< 0,023 x 10^{-2} < 0,114 x 10^{-2} < 0,228 x 10^{-2}
PFH	< 0,047 x 10^{-6}/час	< 0,052 x 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.

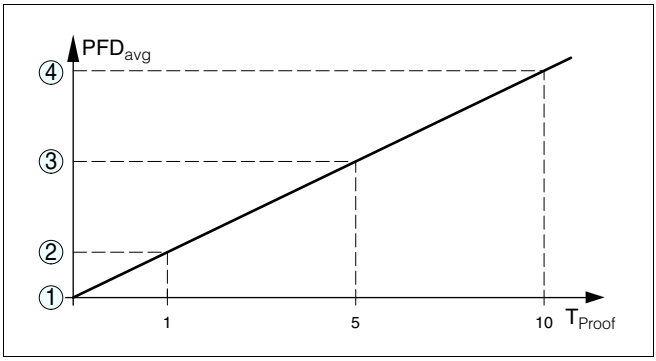


Рис. 1: Изменение PFD_{avg} во времени (числовые значения см. в таблицах выше)

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

exida CERTIFICATION

CERTIFICATE

VEGA 100981C P0011 C001.1

exida Certification S.A. hereby confirms that the

VEGAVIB / VEGAWAVE 60 Level Switch
Output C, R, T, N, Z
Product Version: See listing in assessment report

VEGA Grieshaber KG
Schiltach, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000
Parts 1 - 3, and meets requirements providing a level of integrity to

Systematic Integrity : SIL 3 Capable

Random Integrity : SIL 2 @ HFT=0
SIL 3 @ HFT=1

Safety function
The VEGAVIB / VEGAWAVE 60 will de-energize its output (C,R,T,N) or set current (Z) to fail-safe output when a level goes above (or below) the trip point within the safety accuracy.

Application Restrictions
The unit must be properly designed and validated in a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor

Certifying Assessor

Date: 11 Jan 2011

exida Certification SA, Nyon, Switzerland

Page 1 (2)

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

exida CERTIFICATION

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

Systematic Integrity: SIL 3 Capable

SIL 3 Capability
The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement.

Random Integrity: SIL 2 @ HFT=0
SIL 3 @ HFT=1

Summary for the VEGAVIB / VEGAWAVE 60 Level Switch:
Type B device
IEC 61508 failure rates in FIT [:=10⁻⁹/h]

Model	Fail-Safe state	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
C Max / High trip	Out De-energized	0	506	124	41
C Min / Low trip	Out De-energized	0	481	135	56
R Max / High trip	Out De-energized	0	586	124	27
R Min / Low trip	Out De-energized	0	565	135	37
T Max / High trip	Out De-energized	0	487	124	30
T Min / Low trip	Out De-energized	0	466	135	40
N Max / High trip	Out < 1.0 mA	12	160	390	47
N Min / Low trip	Out < 1.0 mA	36	155	366	52
Z Max / High trip	Out > 12.5 mA	49	387	163	18
Z Min / Low trip	Out < 11.5 mA	39	352	182	43

All failure rates are given in FIT =10^{-9}/h

SIL Verification:
The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH / PFD_{AVG} considering the architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory part of this certificate:
VEGA 03/05-08 R005 V3R1 Assessment Report
Safety manuals VEGAVIB / VEGAWAVE 60, all with versions:
C: 32002 / 32363 R: 32003 / 32364 T: 32004 / 32365
N: 32005 / 32366 Z: 32006 / 32367

The holder of this certificate may use this mark.

exida Certification SA, Nyon, Switzerland

info@exidacert.ch
Page 2 (2)

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.