Safety Manual

VEGACAL серии 60

2-провод. 4 … 20 mA/HART

Document ID: 35593

Содержание

Редакция:2018-11-29

35593-RU-181129

1 Функциональная безопасность

1.1 Общее

Сфера действия

Данное руководство по безопасности действует для измерительных систем с емкостным уровнемером VEGACAL серии 60 в двухпроводном исполнении 4 … 20 mA/HART:

VEGACAL 62, 63, 64, 65, 66, 69

Действительные версии аппаратного и программного обеспечения:

- Серийный номер электроники > 14557661
- Программное обеспечение датчика, версия 1.01 и выше

Область применения

Данная измерительная система может применяться для измерения уровня жидкостей и сыпучих продуктов, удовлетворяющего особым требованиям безопасности.

На основе предшествующего опыта использования, это возможно в одноканальной архитектуре с уровнем полноты безопасности до SIL2, а в многоканальной архитектуре с разнородным резервированием - до SIL3.

Применение измерительной системы в многоканальной архитектуре с однородным резервированием исключается.

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 уровня SIL (IEC 61508-1, 7.6.2)

Уровень полноты 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	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Полнота безопасности аппаратных средств для связанных с безопасностью подсистем типа B (IEC 61508-2, 7.4.3)

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

Проверено в эксплуатации

В соответствии с IEC 61511-1, п. 11.4.4 для подсистем, проверенных предшествующим опытом использования, аппаратная отказоустойчивость HFT может быть уменьшена на один, если выполняются следующие условия:

- Устройство проверено в эксплуатации
- На устройстве могут быть изменены только релевантные 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 управления изменениями явилась составной частью подтверждения предшествующего опыта использования.

1.2 Проектирование

Функция безопасности

Измерительная система производит на токовом выходе соответствующий уровню заполнения сигнал между 3,8 mA и 20,5 mA.

Этот аналоговый сигнал передается на подключенное устройство формирования сигнала для контроля следующих состояний:

- Превышение заданного значения уровня
- Падение ниже заданного значения уровня

При достижении установленных на устройстве формирования сигнала точек переключения выдается сигнал.

Безопасное состояние

Безопасное состояние зависит от режима работы:

	Контроль верхнего уровня	**Контроль нижнего уровня**
Безопасное состояние	Превышение точки переключения	Падение ниже точки переключения
Выходной ток в безопасном состоянии	> Точка переключения (-2 %)	< Точка переключения (+2 %)
Токовый сигнал неисправности "fail low"	< 3,6 mA	< 3,6 mA
Токовый сигнал неисправности "fail high"	> 21,5 mA	> 21,5 mA

Допустимое отклонение тока ±2 % относится к установке 0 … 120 pF (см. Руководство по эксплуатации).

Описание ошибки

Безопасный отказ (safe failure) 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 выходные токи "*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 это не тот случай, то соответствующие части интенсивностей отказов должны быть присвоены опасным отказам. Тем самым могут быть ухудшены числовые значения, указанные в гл. "*Технические показатели безопасности*".

Блок формирования сигнала должен соответствовать уровню SIL измерительной цепи.

Режим работы с низкой частотой запросов

Если частота запросов составляет не более одного раза в год, то измерительная система как часть системы, связанной с безопасностью, может применяться в режиме с "низкой частоты запросов" ("*low demand mode*" по IEC 61508-4, 3.5.12).

Если отношение частоты внутренних диагностических проверок 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} (average Probability of dangerous Failure on Demand, средняя вероятность опасного отказа при запросе). Это значение зависит от интервала T_{Proof} между функциональными проверками функции безопасности.

Числовые значения см. в п. "*Технические показатели безопасности*".

Режим работы с высокой частотой запросов

Если условие "*режима работы с низкой частотой запросов*" не удовлетворяется, то измерительная система как часть системы, связанной с безопасностью, должна применяться в режиме с "высокой частотой запросов" ("*high demand mode*" по IEC 61508-4, 3.5.12).

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

Соответствующим параметром является значение PFH (интенсивность отказов).

Числовые значения см. в п. "*Технические показатели безопасности*".

Допущения

При выполнении анализа видов отказов, влияний и диагностики (FMEDA) были учтены следующие основные условия:

- Интенсивности отказов постоянные, механический износ деталей не учитывается.
- Интенсивности отказов внешних источников питания в расчет не включаются.
- Множественные ошибки не учитываются.
- 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 неисправность и выдавать соответствующий сигнал.

35593-RU-181129

- Чтобы реагировать на опасные обнаруживаемые отказы, интервал опроса подключенного устройства управления и формирования сигнала составляет макс. 1 час
- Имеющиеся коммуникационные интерфейсы (например: HART, I^2C) не используются для передачи релевантных для безопасности данных.

Общие указания и ограничения

Измерительная система должна использоваться соответственно применению с учетом давления, температуры, плотности, диэлектрической постоянной 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:

- Избегать поломки стержня или троса (возможно, потребуются более короткие интервалы между контрольными проверками)

1.3 Параметрирование устройства

Средства настройки

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

Допускаются следующие средства:

- Соответствующий VEGACAL драйвер DTM вместе с программным обеспечением для настройки, соответствующим стандарту FDT/DTM, например PACTware.
- Модуль индикации и настройки

Примечание:
Должна использоваться версия Коллекции DTM 10/2005 или выше.

Установка места измерения

Если измерительная система не была заказана специально для применения в приборной системе безопасности, то в программном обеспечении для настройки в меню "*Базовая установка*" должен быть выбран параметр "*Датчик соотв. SIL*". Если для настройки используется модуль индикации и настройки, то в меню "*Сервис*" нужно активировать параметр "*SIL*".

Состояние при неисправности

Параметрирование тока состояния отказа влияет на технические показатели безопасности. Поэтому для применений, связанных с безопасностью, допускаются только следующие токи состояния отказа:

- fail low = < 3,6 mA (значение по умолчанию)
- fail high = 22 mA

Демпфирование выходного сигнала

Демпфирование выходного сигнала должно соответствовать времени безопасности процесса.

Недопустимые режимы работы

Передача измеренного значения посредством сигнала HART и работа в многоточечном режиме HART не допускаются.

Возможности проверки

Установленные параметры должны проверяться надлежащим способом.

- После подключения устройства к питанию выходной сигнал в конце фазы включения достигает установленного тока состояния отказа.
- В режиме "*Моделирования*" сигнальный ток может моделироваться независимо от действительного уровня.

Блокирование доступа

Для предупреждения непроизвольных или случайных изменений доступ к установленным параметрам должен быть защищен:

- путем активации пароля через программное обеспечение для настройки
- путем активации PIN на модуле индикации и настройки

Доступ с помощью манипулятора HART и т.п. не разрешается.

Защита от случайного или непроизвольного доступа к настройке может быть осуществлена, например, путем блокирования крышки корпуса.

Осторожно!
После выполнения сброса все параметры должны быть проверены или установлены заново.

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 сигналы неисправности описаны в руководстве по эксплуатации.

При обнаружении ошибок или при сигналах неисправности, вся измерительная система должна быть выведена из работы, а безопасное состояние процесса должно поддерживаться другими мерами.

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

35593-RU-181129

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 необнаруженных опасных отказов. 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. "*Технические показатели безопасности*"

При высокой частоте запросов, согласно IEC 61508, периодическая функциональная проверка не предусматривается. Доказательством работоспособности является частое использование измерительной системы. 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.

Если одна из функциональных 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.

1.7 Технические показатели безопасности

Основания

Интенсивности отказов электроники, механических частей датчика и присоединения определены посредством FMEDA в соответствии с IEC 61508. Расчет основан на интенсивностях 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) интенсивности 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 использования

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

Интенсивности отказов

Действительно для защиты от переполнения и сухого хода:

λ_{sd}	0 FIT
λ_{su}	212 FIT
λ_{dd}	458 FIT
λ_{du}	208 FIT
DC_S	0 %
DC_D	68 %
MTBF = MTTF + MTTR	0,93 x 10^6 час

Время реакции на ошибку

E013 (Отсутствует измеренное значение)	< 10 sek.
E036/E037 (Отсутствует исполнимое ПО датчика)	< 1 h

Специфические параметры

Одноканальная архитектура

SIL	SIL2
HFT	0
Тип устройства	Тип B

Действительно для защиты от переполнения и сухого хода:

SFF	76 %
PFD_{avg} T_{Proof} = 1 год T_{Proof} = 5 лет	 < 0,091 x 10^{-2} < 0,182 x 10^{-2}
PFH	< 0,208 x 10^{-6}/час

Ход PFD_{avg} во времени

В пределах 10 лет течение PFD_{avg} во времени приблизительно линейное по отношению ко времени работы. Данные выше значения действительны только для временного интервала T_{Proof}, по истечении которого должна проводиться периодическая функциональная проверка.

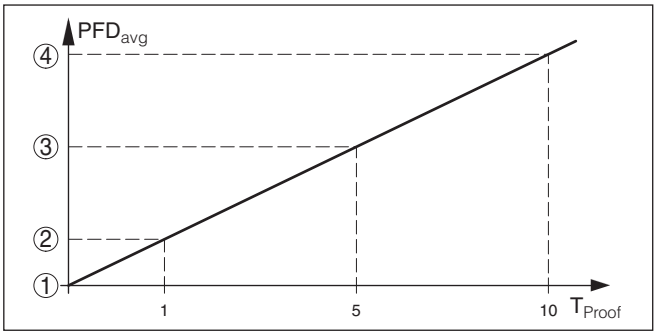

Рис. 1: Ход PFD_{avg} во времени (числовые значения см. в таблицах выше)

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 параметры

При применении измерительной системы в многоканальной архитектуре, технические показатели безопасности выбранной структуры измерительной цепи рассчитываются посредством приведенных выше интенсивностей отказов специально для выбранного применения.

Необходимо учитывать соответствующий фактор общей причины отказов.

Измерительную систему разрешается применять только в архитектуре с разнородным резервированием!

2 Приложение

Konformitätserklärung
Declaration of conformity
Déclaration de conformité

IEC 61508 / IEC 61511

VEGA Grieshaber KG,
Am Hohenstein 113,
77761 Schiltach / Germany

erklärt als Hersteller, dass die kapazitiven Füllstandsensoren der Produktfamilie

declares as manufacturer, that the capacitive level sensors of the product family

déclare en tant que fabricant que les capteurs de niveau capacitifs de la famille

VEGACAL 62, 63, 64, 65, 66, 69

4 ... 20 mA/HART

entsprechend der IEC 61511-1, Abschnitt 11.4.4 („Betriebsbewährtheit“) für den Einsatz in sicherheitsinstrumentierten Systemen (SIS) als Untersystem bis **SIL2** geeignet sind.
Die Sicherheitstechnischen Kennzahlen sowie die Sicherheitshinweise im „Safety Manual“ sind zu beachten.
Die Beurteilung des Änderungswesens war Bestandteil des Nachweises der Betriebsbewährtheit.

according to IEC 61511-1, section 11.4.4 ("proven in use")
are suitable as a subsystem until **SIL2** in safety instrumented systems (SIS).
The safety related characteristics as well as the safety instructions in the ”Safety Manual” must be considered.
The assessment of the modification management was part of the proof for "proven in use".

conviennent à une utilisation dans les systèmes instrumentés de sécurité (SIS) comme sous-système jusqu’à **SIL2** suivant la norme IEC 61511-1, paragraphe 11.4.4 ("validé en utilisation").
Les caractéristiques techniques relatives à la sécurité ainsi que les consignes de sécurité stipulées dans le „Safety Manual“ sont à respecter.
L’évaluation du service de modifications a fait partie de la preuve de la validité en utilisation.

Schiltach, 18 Februar 2009

J. Fehrenbach

Josef Fehrenbach
R&D Director

35593-RU-181129

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

35593-RU-181129

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