Safety Manual
VEGATRENN 149A Ex

Document ID:
35824

Содержание

35824-RU-100219

1 Функциональная безопасность

1.1 Общие положения

Сфера действия

Данное руководство по безопасности действительно для разделителя питания VEGATRENN 149A Ex.

Область применения

Разделитель питания служит для гальванической развязки токовых цепей 4 … 20 mA и питания двухпроводных измерительных преобразователей и может применяться в измерительных цепях с особыми требованиями техники безопасности по IEC 61508/ IEC 61511-1.

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	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
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 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

Датчик, получающий питание от VEGATRENN 149A Ex, производит пропорциональный измеренному значению аналоговый сигнал 4 … 20 mA. Аналоговый сигнал через VEGATRENN 149A Ex доставляется на подключенный логический блок или предельный сигнализатор, где он контролируется на превышение максимального значения или падение ниже минимального значения.

Безопасное состояние

Безопасное состояние зависит от режима работы:

	Контроль верхнего измеренного значения	**Контроль нижнего измеренного значения**
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

Отклонение по току ±2 % допускается относительно полного диапазона измерения 16 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 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 °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 (MTTR = 8 h)

35824-RU-100219

- 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

Система должна быть установлена в соответствии с применением.

Должны соблюдаться предельные значения, установленные для данного применения

Токовая нагрузка выходной цепи должна быть в пределах, соответствующих данным в "Руководстве по эксплуатации".

1.3 Указания по настройке

Элементы настройки

На самом VEGATRENN 149A Ex нет элементов настройки.

Через гнезда HART может осуществляться параметрирование подключенных датчиков. Настройка подключенных датчиков выполняется с помощью ПК с Windows и программным обеспечением для настройки PACTware и DTM.

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

При изменениях во время работы должна соблюдаться функция безопасности.

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

Если из-за обнаруженных ошибок производится замена устройства, то об этом (вместе с описанием ошибок) следует сообщить производителю.

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.

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 сухого хода (min.)	**Защита от переполнения (max.)**	**Диапазон**
λ_{sd}	122 FIT	72 FIT	194 FIT
λ_{su}	122 FIT	122 FIT	122 FIT
λ_{dd}	72 FIT	122 FIT	0 FIT
λ_{du}	63 FIT	63 FIT	63 FIT

MTBF = MTTF + MTTR	2,67 x 10^6 час

Специфические числа

Одноканальная архитектура (1oo1D)

SIL	SIL2
HFT	0
Тип устройства	Тур A

Действительно для защиты от переполнения и сухого хода:

SFF	83 %
PFD_{avg} T_{Proof} = 1 год T_{Proof} = 5 лет	 < 0,028 x 10^{-2} < 0,138 x 10^{-2}
PFH	< 0,063 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.

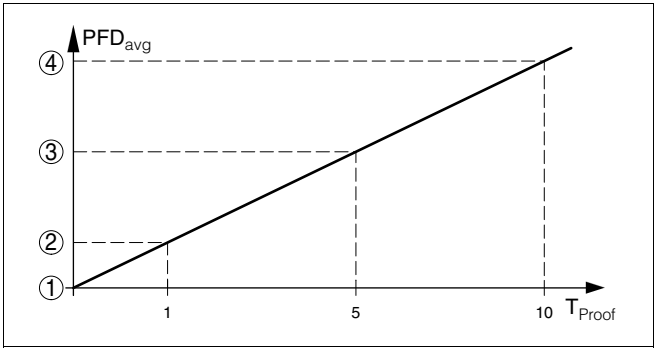

Рис. 1: Изменение PFD_{avg} во времени (числовые значения см. в таблицах выше)

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

FMEDA and Proven-in-use Assessment

Project:
Active Barrier VEGATRENN 149A

Customer:
VEGA Grieshaber KG
Schiltach
Germany

Contract No.: VEGA 08/12-40
Report No.: VEGA 08/12-40 R017
Version V1, Revision R1, January 2009
Stephan Aschenbrenner

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 Active Barrier VEGATRENN 149A.

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.

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. However, as the module under consideration is only one part of an entire safety function it should not claim more than 10% of this range. 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 active barrier would then be 1,00E-03.

The Active Barrier VEGATRENN 149A is considered to be a Type A[1] component 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.

As the Active Barrier VEGATRENN 149A is supposed to be a proven-in-use device, an assessment of the hardware with additional proven-in-use demonstration for the device 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 device is considered to be suitable for use in SIL 2 safety functions.

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 Active Barrier VEGATRENN 149A is used in an application for “low level monitoring”, “high level monitoring” or “range monitoring”. For these applications the following tables show how the above stated requirements are fulfilled.

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

Table 1: Summary for VEGATRENN 149A – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 2,76E-04	PFD_{AVG} = 1,38E-03	PFD_{AVG} = 2,76E-03

Table 2: Summary for VEGATRENN 149A – Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	122 FIT	122 FIT	72 FIT	63 FIT	> 83%	50%	53%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	72 FIT	122 FIT	122 FIT	63 FIT	> 83%	37%	66%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	194 FIT	122 FIT	0 FIT	63 FIT	> 83%	61%	0%

A user of the Active Barrier VEGATRENN 149A 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). The complete list of failure rates is presented in section 5.2 along with all assumptions.

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 10% of this range, i.e. to be better than or equal to 1,00E-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 table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03.

The functional assessment according to IEC 61508 has shown that the Active Barrier VEGATRENN 149A has a PFD_{AVG} 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 a Safe Failure Fraction (SFF) of > 83%. Based on the verification of "prior use" it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

[2] DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for VEGATRENN 149A.

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.