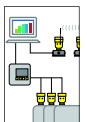


## Safety Manual

### VEGATOR 636 Ex



Document ID:  
32007



## Содержание

<b>1</b>	<b>Функциональная безопасность</b>	
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 . . . . .	7
1.6	Периодическая функциональная проверка . . . . .	7
1.7	Показатели техники безопасности . . . . .	9
<b>2</b>	<b>Приложение</b>	

# 1 Функциональная безопасность

## 1.1 Общие положения

### Сфера действия

Данное руководство по безопасности действительно для устройств формирования сигнала VEGATOR 636Ex.

### Область применения

Устройство формирования сигнала в сочетании с вибрационным сигнализатором уровня может применяться как измерительная система для сигнализации предельного уровня 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 <sub>avg</sub>	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
$\lambda_{sd}$	Rate for safe detected failure
$\lambda_{su}$	Rate for safe undetected failure
$\lambda_{dd}$	Rate for dangerous detected failure
$\lambda_{du}$	Rate for dangerous undetected failure
DC <sub>S</sub>	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd} + \lambda_{su})$
DC <sub>D</sub>	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd} + \lambda_{du})$
FIT	Failure In Time (1 FIT = 1 failure/10 <sup>9</sup> 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 <sub>avg</sub>	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)	(SIL4)
90 % ... < 99 %	SIL3	(SIL4)	(SIL4)	(SIL4)
$\geq 99$ %	SIL3	(SIL4)	(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 состоит в том, что при достижении по запросу процесса заданной точки переключения выходная цепь переключается в обесточенное состояние. Обесточенное состояние выходной цепи зависит от входного тока и режима работы.

**Безопасное состояние** Безопасное состояние зависит от режима работы:

	Защита от переполнения (режим Max/A)	Защита от сухого хода (режим Min/B)
Входной ток в безопасном состоянии	> 12 mA	< 12 mA
Выходная цепь в безопасном состоянии	обесточено	обесточено

Если устройство определяет значение тока < 3,6 mA или > 21,5 mA, оно принимает безопасное состояние.

Безопасным состоянием измерительной системы является разъединенное состояние (принцип тока покоя):

- Релейный выход обесточен
- Транзисторный выход непроводящий

**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** Блок формирования сигнала должен обрабатывать выходную цепь измерительной системы по принципу тока покоя.  
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)
- Блок формирования сигнала обрабатывает выходную цепь измерительной системы по принципу тока покоя
- Чтобы реагировать на опасные обнаруживаемые отказы, интервал опроса подключенного устройства управления и формирования сигнала составляет макс. 1 час

### 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

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

- DIL-переключатель для переключения А/В (режим работы)
- DIL-переключатель для установки задержки выключения/включения
- DIL-переключатель для установки демпфирования (учитывать время нечувствительности к отказам)

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.

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.

### Функциональная проверка в режиме работы "Защита от переполнения"

Если измерительная система применяется для защиты от переполнения, то определение работоспособности обеспечивается путем простой функциональной проверки.

#### Тестовая кнопка:

В случае измерительных установок с сигнализаторами VEGASWING 60 или VEGAVIB 60 с двухпроводным блоком электроники функциональную проверку можно проводить посредством интегрированной тестовой кнопки.

Порядок проверки подробно описан в руководстве по эксплуатации.

### 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**

Данные действительны равным образом для "Защиты от переполнения (режим А)" и для "Защиты от сухого хода (режим В)".

$\lambda_{sd}$	0 FIT
$\lambda_{su}$	509 FIT
$\lambda_{dd}$	0 FIT
$\lambda_{du}$	107 FIT
MTBF = MTTF + MTTR	1,52 x 10 <sup>6</sup> час

**Время реакции на ошибку**

Время реакции на ошибку	< 0,5 сек.
-------------------------	------------

**Одноканальная архитектура (1oo1D)**

**Специфические числа**

SIL	SIL2
HFT	0
Тип устройства	Тип А

SFF	82 %
PFD <sub>avg</sub>	
T <sub>Proof</sub> = 1 год	< 0,047 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 5 лет	< 0,234 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 10 лет	< 0,467 x 10 <sup>-2</sup>

PFH	$< 0,107 \times 10^{-6}/\text{час}$
-----	-------------------------------------

### 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.

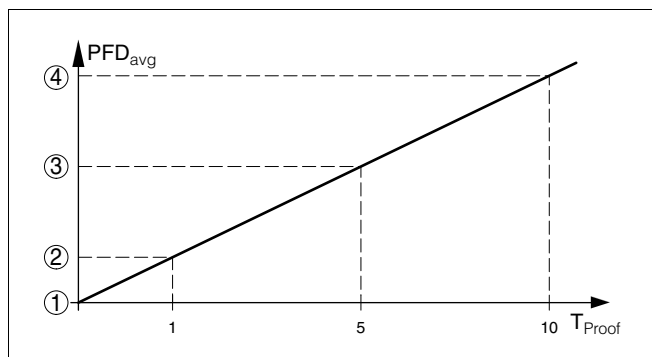


Рис. 1: Изменение  $PFD_{avg}$  во времени (числовые значения см. в таблицах выше)

- 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:

Signal Conditioning Instruments  
VEGATOR 621, VEGATOR 622 and VEGATOR 636  
Applications with level limit detection (MIN / MAX detection)

Customer:

VEGA Grieshaber KG  
Schiltach  
Germany

Contract No.: VEGA 04/08-03  
Report No.: VEGA 04/08-03 R006  
Version V2, Revision R1.1, January 2006  
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 on the format of this technical report 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 signal conditioning instruments VEGATOR 621, VEGATOR 622 and VEGATOR 636.

VEGATOR 621, VEGATOR 622 and VEGATOR 636 are equipped with relay output and transistor output. The results given in this report represent the worst-case output with regard to the dangerous undetected failure rate.

The failure rates used in this analysis are the basic failure rates from 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. For systems operating in high demand mode of operation the PFH value has to be  $\geq 10^{-7}$  1/h to  $< 10^{-6}$  1/h for SIL 2 safety functions according to table 3 of IEC 61508-1. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to 1,00E-03 and 1,00E-07 1/h respectively.

The signal conditioning instruments VEGATOR 621, VEGATOR 622 and VEGATOR 636 are considered to be Type A<sup>1</sup> components with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 60% and 90% according to table 2 of IEC 61508-2 for SIL 2 (sub-) systems with a hardware fault tolerance of 0.

**Table 1: Summary VEGATOR 621 – Failure rates according to IEC 61508**

$\lambda_{\text{safe}}$	$\lambda_{\text{dangerous}}$	SFF
505 FIT	137 FIT	78%

**Table 2: Summary VEGATOR 621 – PFD<sub>AVG</sub> / PFH values**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 1,37E-07 1/h <sup>2</sup>	PFD <sub>AVG</sub> = 6,00E-04	PFD <sub>AVG</sub> = 2,99E-03	PFD <sub>AVG</sub> = 5,98E-03

**Table 3: Summary VEGATOR 622 – Failure rates according to IEC 61508**

$\lambda_{\text{safe}}$	$\lambda_{\text{dangerous}}$	SFF
506 FIT	167 FIT	75%

**Table 4: Summary VEGATOR 622 – PFD<sub>AVG</sub> / PFH values**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 1,67E-07 1/h <sup>2</sup>	PFD <sub>AVG</sub> = 7,32E-04	PFD <sub>AVG</sub> = 3,65E-03	PFD <sub>AVG</sub> = 7,29E-03

<sup>1</sup> Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

<sup>2</sup> The PFH value is based on a fault reaction time of 200 ms. This also requires that a connected logic solver or actuator is able to react within the process safety time.



**Table 5: Summary VEGATOR 636 – Failure rates according to IEC 61508**

$\lambda_{safe}$	$\lambda_{dangerous}$	SFF
509 FIT	107 FIT	82%

**Table 6: Summary VEGATOR 636 – PFD<sub>AVG</sub> / PFH values**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 1,07E-07 1/h <sup>3</sup>	PFD <sub>AVG</sub> = 4,69E-04	PFD <sub>AVG</sub> = 2,34E-03	PFD <sub>AVG</sub> = 4,67E-03

The boxes marked in yellow (■) mean that the calculated PFD<sub>AVG</sub> / PFH values are within the allowed range for SIL 2 according to table 2 / 3 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 and 1,00E-07 1/h respectively. The boxes marked in green (■) mean that the calculated PFD<sub>AVG</sub> / PFH values are within the allowed range for SIL 2 according to table 2 / 3 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 and 1,00E-07 1/h respectively.

Because the Safe Failure Fraction (SFF) is above 60%, also the architectural constraints requirements of table 2 of IEC 61508-2 for Type A subsystems with a Hardware Fault Tolerance (HFT) of 0 are fulfilled.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the signal conditioning instruments VEGATOR 621, VEGATOR 622 and VEGATOR 636 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 is presented in section 5.1 to 5.3 along with all assumptions.

The failure rates are valid for the useful life of the signal conditioning instruments VEGATOR 621, VEGATOR 622 and VEGATOR 636, which is estimated to be between 8 and 12 years (see Appendix 2).

It is important to realize that the "no effect" failures and the "annunciation" failures are included in the "safe" failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

<sup>3</sup> The PFH value is based on a fault reaction time of 200 ms. This also requires that a connected logic solver or actuator is able to react within the process safety time.







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](http://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