

ПРЕОБРАЗОВАТЕЛИ ТЕМПЕРАТУРЫ ВТОРИЧНЫЕ
ИСКРОБЕЗОПАСНЫЕ ЛПА-350
Руководство по функциональной безопасности

Оглавление

1. Общие сведения	3
2. Сфера действия	3
2.1 Исполнение устройства.....	3
2.2 Область применения.....	3
3. Проектирование	4
3.1 Режимы работы.....	4
3.2 Необходимые условия для правильной эксплуатации	4
3.3 Функция безопасности и безопасное состояние	5
4. Показатели функциональной безопасности	6
4.1 Показатели функциональной безопасности в соответствии с ГОСТ Р МЭК 61508.....	6
4.2 Дополнительные сведения	7
5. Запуск в эксплуатацию.....	8
5.1 Общее.....	8
6. Диагностика и обслуживание	11
6.1 Контроль параметров на объекте	11
6.2 Ремонт.....	12
7. Контрольная проверка	12
Приложение А - Протокол проверки.....	14
Приложение В – Определения.....	15

1. Общие сведения

Данное руководство по функциональной безопасности разработано в соответствии с ГОСТ Р МЭК 61508-2-2012.

Цель руководства по безопасности для состоит в документальном оформлении информации, связанной с применяемыми преобразователями температуры вторичными искробезопасными ЛПА-350, которая необходима для обеспечения интеграции применяемого изделия в связанную с безопасностью систему, или подсистему, или элемент в соответствии с требованиями ГОСТ Р МЭК 61508-2-2012.

2. Сфера действия

2.1 Исполнение устройства

Данное руководство по безопасности действует для преобразователей температуры вторичных искробезопасных ЛПА-350 (в дальнейшем преобразователей). Преобразователи с искробезопасными электрическими цепями уровня "ia" выполнены в соответствии с требованиями ГОСТ 31610.11-2014, ГОСТ 31610.0-2014, имеют маркировки взрывозащиты «[Ex ia Ga] IIC», «[Ex ia Ga] IIB», [Ex ia Da] IIC, [Ex ia Ma] I и предназначены для установки вне взрывоопасных зон.

Обозначение исполнений преобразователей имеет следующий вид:

ЛПА-350-АВС



Данный вид обозначения следует применять при заказе преобразователей.

Внимание: Исполнения ЛПА-350-21Х (два входа, один выход) не выпускаются.

2.2 Область применения

Преобразователи предназначены для приема, преобразования и линеаризации сигналов от термопреобразователей сопротивления (ТС) и термопар (ТП), сигналов сопротивления и напряжения постоянного тока, выдачи выходных унифицированных аналоговых сигналов, обеспечения связи по интерфейсу RS-485, а также для обеспечения искробезопасности электрических цепей устройств, устанавливаемых во взрывоопасных зонах помещений и наружных установок.

Преобразователи являются программно-конфигурируемыми изделиями. Подробные технические характеристики и возможности конфигурирования преобразователей

изложены в руководстве по эксплуатации «Преобразователи температуры вторичные искробезопасные ЛПА-350 ОЛПА-21.018.30 РЭ»

Обновление встроенного программного обеспечения преобразователя осуществляется с помощью программы «Конфигуратор ЛПА». При обновлении программного обеспечения преобразователя следует руководствоваться документом «Конфигуратор ЛПА. Руководство пользователя» (доступен на сайте производителя lpadevice.ru).

3. Проектирование

3.1 Режимы работы

Преобразователи могут применяться в связанных с безопасностью системах, в соответствии с ГОСТ Р МЭК 61508, в режимах работы low demand mode (с низкой частотой запросов) или high demand mode (с высокой частотой запросов):

3.2 Необходимые условия для правильной эксплуатации

- Должны выдерживаться границы условий эксплуатации, указанные в руководстве по эксплуатации «Преобразователи температуры вторичные искробезопасные ЛПА-350 ОЛПА-21.018.30 РЭ»;
- Версии программного обеспечения преобразователя и программы «Конфигуратор ЛПА» должны быть актуальными. Актуальные версии ПО доступны на сайте производителя lpadevice.ru;
- Должны быть приняты во внимание указания к главе 4.2;
- Должны использоваться только схемы подключения, приведенные в главе 5;
- К клеммам неиспользуемых входов и выходов не должно подключаться никаких линий связи (проводов);
- Все составные части измерительной цепи должны соответствовать предусмотренному уровню полноты безопасности "Safety Integrity Level (SIL)";
- Преобразователи не защищены от сбоев электропитания. В обязанности пользователя входит обеспечение обнаружения низкого напряжения питания преобразователей и адекватной реакции на эту неисправность;
- Аппаратура и программное обеспечение системы ПАЗ должны быть способны обнаруживать выход сигнала за пределы рабочего диапазона: $I_{out} < 3,6 \text{ мА}$ и $I_{out} > 21 \text{ мА}$ (соответствует стандарту NAMUR NE43);
- Выход(ы) преобразователя должен(ы) быть сконфигурирован(ы) на диапазон выходного сигнала 4...20 мА.

Для FMEDA анализа по с ГОСТ Р МЭК 61508 были сделаны следующие допущения:

- Для двухканального исполнения преобразователя только 1 канал может быть частью функции безопасности;
- Преобразователь ЛПА-350-12х можно использовать в двух вариантах:
 - а) в функции безопасности используется только один выход (1oo1);
 - б) в функции безопасности используются оба выхода, при этом оба выхода подключены к одной системе ПАЗ (1oo2).
- Значения интенсивностей отказов компонентов взяты из баз данных по надёжности Siemens SN 29500-2016, Telcordia Issue 4, Component Reliability Database (CRD) Exida;
- Значения интенсивностей отказов компонентов являются постоянной величиной, механизмы естественного износа не учитываются;

- Распространение отказов не рассматривается;
- Преобразователи отнесены к типу В по ГОСТ Р МЭК 61508-1-2012 с отказоустойчивостью аппаратных средств $HFT=0$;
- Среднее время ремонта $MTTR$ преобразователей составляет 8 часов;
- На время ремонта преобразователя принимаются необходимые меры для сохранения функции безопасности (например, с помощью запасного преобразователя);
- Отказы, возникающие в процессе задания параметров не рассматриваются;
- Не рассматривается использование датчиков с НСХ отличной от указанной в конфигурации преобразователя, неверное задание диапазонов преобразования и прочие ошибки конфигурирования преобразователя.
- Отказом преобразователя считается невозможность выполнения заявленной функции безопасности;
- Приведенные интенсивности отказов соответствуют рабочему диапазону температур $-40...+70^{\circ}\text{C}$ и относительной влажности до 90 % при 35°C и более низких температурах без конденсации влаги при средней температуре за длительный период времени 40°C . В случае более высокой средней температуры 60°C интенсивности отказов должны быть умножены на поправочный коэффициент 2,5, полученный на основе статистики. Подобный коэффициент должен использоваться, если имеют место частые изменения температуры.

SIL2

- В режиме с низкой частотой запросов общее значение PFD_{avg} должно быть меньше 10^{-2} , следовательно, максимально допустимое значение PFD_{avg} будет равно 10^{-3} ;
- В режиме с высокой частотой запросов общее значение PFH должно быть меньше 10^{-6} , следовательно, максимально допустимое значение PFH будет равно 10^{-7} ;
- Поскольку отказоустойчивость аппаратных средств равна 0 и преобразователь является компонентом типа В, доля безопасных отказов компонентов SFF должна быть больше 90% в соответствии с таблицей 2 стандарта ГОСТ Р МЭК 61508-2 для системы SIL2.

3.3 Функция безопасности и безопасное состояние

Функцией безопасности является преобразование и линеаризация входного аналогового от ТС или ТП в выходной аналоговый сигнал 4...20 мА с точностью не хуже 2% за время не более 3-х циклов преобразования АЦП (см. «Преобразователи температуры вторичные искробезопасные ЛПА-350 ОЛПА-21.018.30 РЭ»).

Безопасное состояние: выход сигнала за пределы рабочего диапазона $I_{out} < 3,6 \text{ мА}$ и $I_{out} > 21 \text{ мА}$ (соответствует стандарту NAMUR NE43).

Отказы, приводящие к выходу сигнала за границы рабочего диапазона, относятся к опасным обнаруживаемым отказам λ_{dd} . Отказы, при которых сигнал остается в пределах границ рабочего диапазона, но погрешность которого составляет более 2%, относятся к опасным не обнаруживаемым отказам λ_{du} .

4. Показатели функциональной безопасности

4.1 Показатели функциональной безопасности в соответствии с ГОСТ Р МЭК 61508

Таблица 1. Показатели безопасности преобразователя в режиме приема сигнала от термопреобразователей сопротивления.

Показатель	ЛПА-350-220(221)	ЛПА-350-110(111)	ЛПА-350-120(121) 1 выход (1oo1)	ЛПА-350-120(121) 2 выхода (1oo2)
Уровень полноты безопасности (Safety Integrity Level)	SIL2	SIL2	SIL2	SIL2
Устойчивость к отказам аппаратных средств	HFT = 0			
Тип устройства	Тип В			
Режим работы	С низкой частотой запросов, с высокой частотой запросов			
SFF	91,38	90,67	90,46	90,85
λ_{DU}	73 FIT	72,3 FIT	72,1 FIT	72,4 FIT
λ_{DD}	774 FIT	702 FIT	684 FIT	710 FIT
λ_{SD}	0	0	0	8,63 FIT
λ_{SU}	0	0	0	0
PFH*	$7,3 \cdot 10^{-8}$	$7,23 \cdot 10^{-8}$	$7,21 \cdot 10^{-8}$	$8,6 \cdot 10^{-9}$
PFD_{avg} (T _{proof} = 1 год)	$3,27 \cdot 10^{-4}$	$3,23 \cdot 10^{-4}$	$3,22 \cdot 10^{-4}$	$3,22 \cdot 10^{-5}$
PFD_{avg} (T _{proof} = 3 года)	$9,67 \cdot 10^{-4}$	$9,56 \cdot 10^{-4}$	$9,54 \cdot 10^{-4}$	$9,71 \cdot 10^{-5}$
PFD_{avg} (T _{proof} = 5 года)	$1,61 \cdot 10^{-3}$	$1,59 \cdot 10^{-3}$	$1,59 \cdot 10^{-3}$	$1,63 \cdot 10^{-4}$
PFD_{avg} (T _{proof} = 10 года)	$3,21 \cdot 10^{-3}$	$3,17 \cdot 10^{-3}$	$3,17 \cdot 10^{-3}$	$3,35 \cdot 10^{-4}$
Средняя наработка до отказа (MTTF)*, ч	477289	709201	658517	
Среднее время восстановления (MTTR), ч	8			
Средняя наработка между отказами (MTBF), ч	477297	709209	658525	

* - "Зеленым цветом выделены значения PFH и PFDavg, которые занимают $\leq 10\%$ от общего количества опасных отказов для SIL2 контура безопасности. Желтым цветом выделены значения PFH и PFDavg, которые занимают $> 10\%$ от общего количества опасных отказов для SIL2 контура безопасности."

Таблица 2. Показатели безопасности преобразователя в режиме приема сигнала от термопар.

Показатель	ЛПА-350-220(221)	ЛПА-350-110(111)	ЛПА-350-120(121) 1 выход (1001)	ЛПА-350-120(121) 2 выхода (1002)
Уровень полноты безопасности (Safety Integrity Level)	SIL2	SIL2	SIL2	SIL2
Устойчивость к отказам аппаратных средств	HFT = 0			
Тип устройства	Тип В			
Режим работы	С низкой частотой запросов, с высокой частотой запросов			
SFF	91,01	90,3	90,08	90,49
λ_{DU}	76,4 FIT	75,6 FIT	75,4 FIT	75,6 FIT
λ_{DD}	773 FIT	703 FIT	685 FIT	711 FIT
λ_{SD}	0	0	0	8,63 FIT
λ_{SU}	0	0	0	0
PFH*	$7,64 \cdot 10^{-8}$	$7,56 \cdot 10^{-8}$	$7,54 \cdot 10^{-8}$	$7,6 \cdot 10^{-9}$
$PFD_{avg} (T_{proof} = 1 \text{ год})$	$3,41 \cdot 10^{-4}$	$3,37 \cdot 10^{-4}$	$3,36 \cdot 10^{-4}$	$3,37 \cdot 10^{-5}$
$PFD_{avg} (T_{proof} = 3 \text{ года})$	$1,01 \cdot 10^{-3}$	$9,99 \cdot 10^{-4}$	$9,96 \cdot 10^{-4}$	$1,02 \cdot 10^{-4}$
$PFD_{avg} (T_{proof} = 5 \text{ года})$	$1,68 \cdot 10^{-3}$	$1,66 \cdot 10^{-3}$	$1,66 \cdot 10^{-3}$	$1,71 \cdot 10^{-4}$
$PFD_{avg} (T_{proof} = 10 \text{ года})$	$3,35 \cdot 10^{-3}$	$3,32 \cdot 10^{-3}$	$3,31 \cdot 10^{-3}$	$3,51 \cdot 10^{-4}$
Средняя наработка до отказа (MTTF)*, ч	477289	709201	658517	
Среднее время восстановления (MTTR), ч	8			
Средняя наработка между отказами (MTBF), ч	477297	709209	658525	

* - "Зеленым цветом выделены значения PFH и PFDavg, которые занимают $\leq 10\%$ от общего количества опасных отказов для SIL2 контура безопасности. Желтым цветом выделены значения PFH и PFDavg, которые занимают $> 10\%$ от общего количества опасных отказов для SIL2 контура безопасности."

4.2 Дополнительные сведения

Доля безопасных отказ SFF была рассчитана по следующей формуле:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Значения PFD_{AVG} для архитектуры 1001 были рассчитаны следующим образом:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_{proof}}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_{avg} = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

Значения PFD_{AVG} для архитектуры 1002 были рассчитаны следующим образом:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_{proof}}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_{proof}}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_{avg} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{GE} t_{CE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_{proof}}{2} + MRT \right)$$

$$PFH_{1002} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})(1 - \beta)\lambda_{DU} t_{CE} + \beta \lambda_{DU}$$

β – доля необнаруженных отказов по общей причине, принято 10%;

β_D – доля отказов, обнаруженных диагностическими тестами и имеющих общую причину, принято 5%;

t_{CE} – эквивалентное среднее время простоя канала для архитектур 1001, 1002, 2002 и 2003;

t_{GE} – эквивалентное среднее время простоя голосующей группы для архитектур 1001, 1002, 2002 и 2003;

λ_{DU} – интенсивность необнаруженных опасных отказов;

λ_{DD} – интенсивность обнаруженных опасных отказов;

λ_{SU} – интенсивность необнаруженных безопасных отказов;

λ_{SD} – интенсивность обнаруженных безопасных отказов;

T_{proof} – время между проведением проверочных диагностических тестов;

$MTTR$ – среднее время, необходимое для восстановления нормальной работы после возникновения отказа, принято 8ч;

MRT – средняя продолжительность нахождения устройства в неработоспособном состоянии, обусловленном его ремонтом, принято 8ч.

5. Запуск в эксплуатацию

5.1 Общее

Требуется выполнять содержащиеся в руководстве по эксплуатации «Преобразователи температуры вторичные искробезопасные ЛПА-350 ОЛПА-21.018.30 РЭ» рекомендации по монтажу и подключению преобразователя.

Сведения по конфигурированию преобразователей приведены в руководстве по эксплуатации «Преобразователи температуры вторичные искробезопасные ЛПА-350 ОЛПА-21.018.30 РЭ». При конфигурировании преобразователя следует руководствоваться документом «Конфигуратор ЛПА. Руководство пользователя».

Схемы подключения преобразователей, допустимые для выполнения функции безопасности, приведены ниже.

Внимание: Преобразователи необходимо сконфигурировать для работы с применяемой схемой подключения.

На схемах ниже показаны подключения к входным цепям преобразователей ЛПА-350-2ХХ. Подключения к преобразователям ЛПА-350-1ХХ отличаются тем, что отсутствует второй вход.

На схемах подключения использованы следующие обозначения:

Rt1, Rt2 – Термопреобразователи сопротивления (датчики).

Tc1, Tc2 – Термодпары.

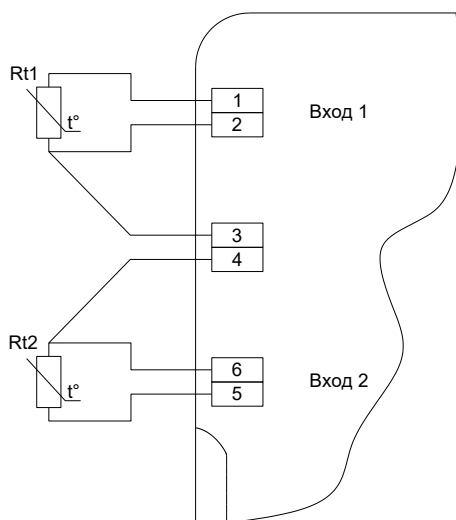


Рисунок 5-1 Схема подключения термопреобразователей сопротивления к преобразователям ЛПА-350-2ХХ по 3-проводной схеме.

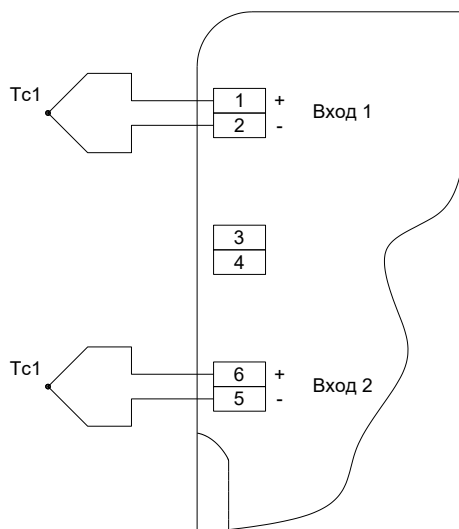


Рисунок 5-2 Схема подключения термодпар к преобразователям ЛПА-350-2ХХ

На схемах ниже показаны подключения к выходным цепям преобразователей ЛПА-350-Х2Х. Подключения к преобразователям ЛПА-350-Х1Х отличаются тем, что отсутствует второй выход.

На схемах подключения использованы следующие обозначения:

R1, R2 – Сопротивления нагрузки.

Внимание: Выходы преобразователя являются активными и рассчитаны на работу исключительно с пассивной нагрузкой.

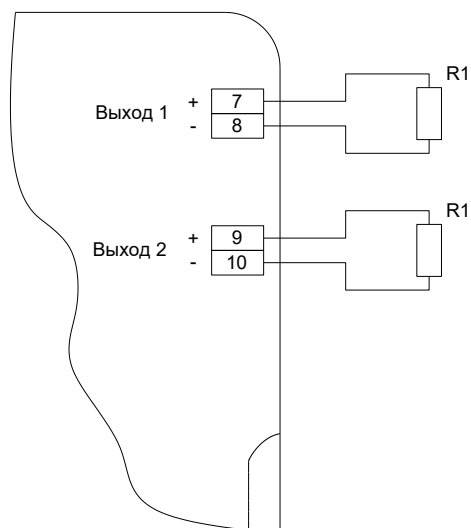


Рисунок 5-3 Схема подключения преобразователя ЛПА-350-Х2Х для сигналов постоянного тока 4...20 мА с отдельной нагрузкой.

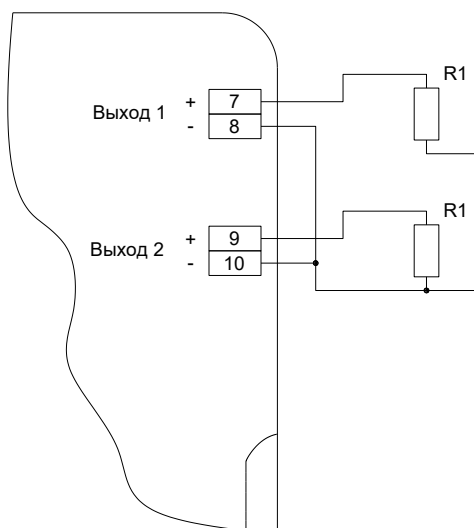


Рисунок 5-4 Схема подключения преобразователя ЛПА-350-Х2Х для сигналов постоянного тока 4...20 мА с нагрузкой, объединенной по общему проводу.

На схемах ниже показаны варианты подключения питания к преобразователям.

На схемах подключения использованы следующие обозначения:

БП – Блок питания.

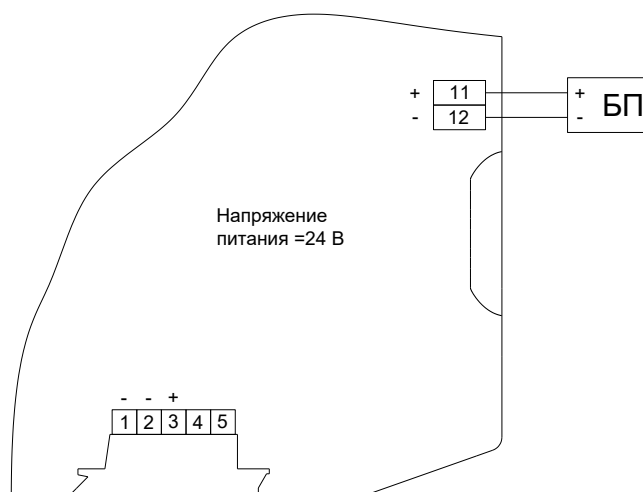


Рисунок 5-5 Схема подключения питания преобразователя ЛПА-350-XXX через клеммные колодки.

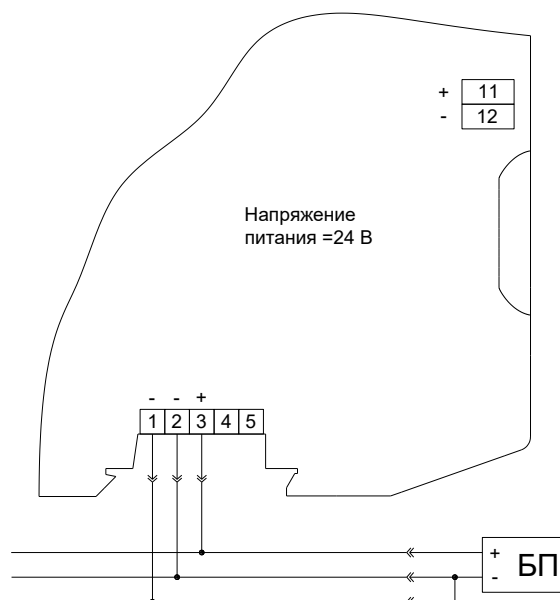


Рисунок 5-6 Схема подключения питания преобразователя ЛПА-350-XXX через шину T-BUS.

В случае установки на объединительные модули ЛПА-300 преобразователи получают напряжение питания непосредственно с модуля. Информация по подключениям питания изложена в документации на модули ЛПА-300.

6. Диагностика и обслуживание

6.1 Контроль параметров на объекте

В соответствии с ГОСТ Р МЭК 61508-2-2012 на объекте должны периодически проводится контрольные проверки, подтверждающие правильное выполнение функции безопасности.

Выбор вида проверки является ответственностью лица, эксплуатирующего устройство. Временные интервалы между проверками выбираются, руководствуясь

требуемой средней вероятностью опасных ошибок по запросу PFD_{AVG} (см. 4.1 Показатели функциональной безопасности в соответствии с ГОСТ Р МЭК 61508).

Для документирования проверки может использоваться форма протокола проверки, показанная в Приложении А.

Если одна из проверок протекает отрицательно, то вся измерительная система должна быть выведена из работы, а безопасное состояние процесса должно поддерживаться другими мерами.

Внимание!

Во время функционального теста функция безопасности должна рассматриваться как небезопасная. Следует учитывать, что функциональный тест оказывает влияние на подключенные устройства.

При необходимости, должны предприниматься другие меры для поддержания функции безопасности.

После завершения функционального теста должно быть восстановлено состояние, определенное для функции безопасности.

6.2 Ремонт

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

О появлении опасной необнаруженной ошибки следует сообщить производителю (с приложением описания ошибки).

При выходе из строя преобразователя для его ремонта необходимо обратиться к производителю.

7. Контрольная проверка

Для обнаружения возможных опасных необнаруженных ошибок, функция безопасности должна проверяться через соответствующие промежутки времени посредством контрольной проверки. Выбор вида проверки является ответственностью лица, эксплуатирующего устройство. Временные интервалы между проверками выбираются, руководствуясь требуемой средней вероятностью опасных ошибок по запросу PFD_{AVG} (см. гл. " 4. Показатели функциональной безопасности ").

Для документирования этой проверки может использоваться форма протокола проверки, показанная в Приложении А.

Если одна из проверок протекает отрицательно, то вся измерительная система должна быть выведена из работы, а безопасное состояние процесса должно поддерживаться другими мерами.

Внимание!

Во время функционального теста функция безопасности должна рассматриваться как небезопасная. Следует учитывать, что функциональный тест оказывает влияние на подключенные устройства.

При необходимости, должны предприниматься другие меры для поддержания функции безопасности.

После завершения функционального теста должно быть восстановлено состояние, определенное для функции безопасности.

Процедура № 1: устройство остается в смонтированном состоянии и есть возможность задания (имитации) входного сигнала.

Процедура № 2: устройство демонтировано и есть возможность проведения теста с помощью соответствующих устройств и приборов.

Для этого необходимо

Последовательно подать значения входного сигнала, соответствующие 0%; 25%; 50% 75% и 100% сконфигурированного входного диапазона преобразования. Справочные значения входного сигнала и соответствующие ожидаемые значения выходного сигнала можно получить в программе «Конфигуратор ЛПА».

Ожидаемые результаты:

Значения выходного сигнала преобразователя соответствуют поданным значениям входного сигнала с погрешностью не более $\pm 2\%$ от диапазона выходного сигнала.

Охват проверки

Остающиеся опасные необнаруженные ошибки составляют 72-76 FIT ($\beta = 95\%$)

Приложение А - Протокол проверки

Идентификация	
Фирма/Проверяющее лицо	
Тип устройства/Код заказа	
Серийный номер устройства	
Дата начальной установки	
Дата последней проверки Функции безопасности	

Основание/объем проверки	
	Начальная установка преобразователя
	Контроль параметров преобразователя на объекте
	Контрольная проверка с демонтажом преобразователя

Результат проверки			
Значение входного сигнала	Допустимый диапазон выходного сигнала	Измеренное значение выходного сигнала	Результат проверки
	3,68...4,32 мА		
	7,68...8,32 мА		
	11,68...12,32 мА		
	15,68...16,32 мА		
	19,68...20,32 мА		

Дата:	Подпись:
-------	----------

Приложение В – Определения

Функциональная безопасность (Functional Safety) – часть общей системы безопасности, обусловленная применением управляемого оборудования и системы управления и зависящая от правильности функционирования электрических/электронных/программируемых электронных систем, связанных с безопасностью, и других средств по снижению риска.

ПАЗ – противоаварийная защита.

ДБО (SFF – safety fail fraction) – Доля Безопасных Отказов. Свойство элемента, связанного с безопасностью, определяемое отношением суммы средних частот безопасных отказов и опасных обнаруженных отказов к сумме средних частот безопасных и опасных отказов.

λ_{du} – интенсивность необнаруженных опасных отказов.

λ_{dd} – интенсивность обнаруженных опасных отказов.

λ_{su} – интенсивность необнаруженных безопасных отказов.

λ_{sd} – интенсивность обнаруженных безопасных отказов.

ОАС (HFT – hardware fault tolerance) – Отказоустойчивость Аппаратных Средств.

ОАС = X означает, что X+1 является минимальным числом отказов, которые могут привести к потере функции безопасности.

Средняя вероятность опасного отказа по запросу (probability of dangerous failure on demand, PFDavg) – средняя неготовность Э/Э/ПЭ системы, связанной с безопасностью, обеспечить безопасность, т.е. выполнить указанную функцию безопасности, когда происходит запрос.

Средняя частота опасного отказа в час (average frequency of a dangerous failure per hour, PFH)

– средняя частота опасного отказа Э/Э/ПЭ системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.

Полнота безопасности (safety integrity) – вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного периода времени.

УПБ (SIL – safety integrity level) – Уровень полноты безопасности: дискретный уровень (принимаящий одно из четырёх значений), определяющий требования к полноте безопасности для функции безопасности, который ставится в соответствии с Э/Э/ПЭС системам, связанным с безопасностью.

Средняя наработка до отказа (MTTF = Mean Time To Failure) – наработка объекта от начала эксплуатации до возникновения первого отказа

Средняя наработка между отказами (MTBF – Mean Time Between Failures) – наработка объекта от окончания восстановления его работоспособного состояния после отказа до возникновения следующего отказа.

Среднее время восстановления (MTTR – Mean Time To Restoration) – среднее время, необходимое для восстановления нормальной работы после возникновения отказа.

Среднее время ремонта (MRT Mean Repair Time) – средняя продолжительность нахождения устройства в неработоспособном состоянии, обусловленном его ремонтом.

β – доля необнаруженных отказов по общей причине.

β_D – доля отказов, обнаруженных диагностическими тестами и имеющих общую причину.

t_{CE} – эквивалентное среднее время простоя канала для архитектур 1oo1, 1oo2, 2oo2 и 2oo3.

t_{GE} – эквивалентное среднее время простоя голосующей группы для архитектур.