ЭЛЕМЕР

ООО НПП "ЭЛЕМЕР"

РОССИЙСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ЗАВОД

ПРЕОБРАЗОВАТЕЛИ ДАВЛЕНИЯ ИЗМЕРИТЕЛЬНЫЕ АИР-10SH

Руководство по функциональной безопасности

НКГЖ.406233.052ФБ

СОДЕРЖАНИЕ

1 Общие сведения

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

Цель руководства по безопасности состоит в документальном оформлении информации, связанной с применяемыми преобразователями давления измерительными АИР-10SH (далее – АИР-10SH), которая необходима для обеспечения интеграции применяемого изделия в систему, или подсистему, или элемент, связанные с безопасностью, в соответствии с требованиями ГОСТ Р МЭК 61508-2-2012.

2 Сфера действия

2.1 Исполнение устройства

Данное руководство по безопасности распространяется на АИР-10SH исполнений АИР-10SH, АИР-10SH ОМ, АИР-10ASH, АИР-10ASH ОМ, АИР-10AExSH, АИР-10AExSH ОМ, АИР-10AExdSH, АИР-10AExdSH ОМ, пяти модификаций АИР-10SH-ДА, АИР-10SH-ДИ, АИР-10SH-ДИВ, АИР-10SH-ДД, АИР-10SH-ДГ, отличающихся измеряемым параметром. Подробное описание исполнений и модификаций АИР-10SH изложено в руководстве по эксплуатации НКГЖ.406233.052РЭ.

2.2 Область применения

АИР-10SH предназначены для непрерывного преобразования значений абсолютного давления, избыточного давления, избыточного давления-разрежения, разности давлений жидких и газообразных, в том числе агрессивных, сред, в унифицированный выходной токовый сигнал 4-20 мА и в цифровой сигнал на базе HART-протокола.

Выходные сигналы АИР-10SH соответствуют приведенным в таблице 1.

Таблица 1 – Код выходного сигнала

Код при заказе	Выходной сигнал	Зависимость выходного сигнала от входного
42	4-20 мА	линейно-возрастающая
24	20-4 мА	линейно-убывающая
42√	4-20 мА	корнеизвлекающая

Изделие может 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):

До SIL2 в одноканальной архитектуре.

3 Проектирование

3.1 Функция безопасности и безопасное состояние

Функцией безопасности является корректное отображение действующего значения давления рабочей среды в единицах выходного сигнала.

3.2 Необходимые условия для правильной эксплуатации

- Должны выдерживаться границы условий применения, указанные в руководстве по эксплуатации. Не допускается применение АИР-10SH для измерения параметров сред, агрессивных по отношению к материалам, контактирующим с измеряемой средой.
- Спецификации согласно данным руководства по эксплуатации, особенно токовая нагрузка выходной цепи, должны выдерживаться в указных пределах.
- Должны быть приняты во внимание дополнительные сведения, указанные в главе 4.2.

- Все составные части измерительной цепи должны соответствовать предусмотренному уровню полноты безопасности "Safety Integrity Level (SIL)".

4 Показатели функциональной безопасности

4.1 Показатели в соответствии с ГОСТ Р МЭК 61508

Таблица 2 – Показатели функциональной безопасности

Показатель	Значение
Уровень полноты безопасности (Safety Integrity Level)	УПБ2 (SIL2)
Устойчивость к отказам аппаратных средств	HFT = 0
Тип устройства	B
Режим работы	С низкой частотой запросов; с высокой частотой запросов
ДБО (SFF)	92 %
λsd	90 FIT
λsu	31 FIT
λdd	280 FIT
λdu	35 FIT
PFDavg	$0,6 \cdot 10^{-3}$ (T_{Proof} = 1 год) для среднего срока службы 30 лет; $0,37 \cdot 10^{-3}$ (T_{Proof} = 1 год) для среднего срока службы 15 лет
PFH	$1,75 \cdot 10^{-7}$/час

4.2 Дополнительные сведения

Частоты отказов устройства определяются посредством FMEDA анализа по ГОСТ Р МЭК 61508.

В основе расчетов лежат частоты отказов конструктивных элементов по SN 29500. Следующие исходные предпосылки были сделаны при анализе видов, эффектов и диагностики отказов АИР-10SH:

- Интенсивность отказов является постоянной величиной, механизмы естественного износа не учитываются. Распространение отказов не рассматривается.
- Износ механических частей не учитывается.
- Отказы, возникающие в процессе задания параметров, не рассматриваются.
- АИР-10SH относятся к компоненту типа B по ГОСТ Р МЭК 61508-1-2012.
- Отказом АИР-10SH считается невозможность выполнения заявленных функций.
- Среднее время восстановления MTTR АИР-10SH составляет 8 ч.
- Интенсивность отказов внешнего источника питания не учитывалась.
- Приведенные интенсивности отказов соответствуют типичным условиям эксплуатации на промышленных предприятиях, описанным в стандарте МЭК 60654-1, класс С, при средней температуре за длительный период времени 40 °С. В случае более высокой средней температуры (80 °С) интенсивности отказов должны быть умножены на поправочный коэффициент 2.5, полученный на основе статистики. Подобный коэффициент должен использоваться, если имеют место частые изменения температуры.

Приведенные выше значения для PFD_{avg} были рассчитаны для архитектуры 1oo1 следующим образом:

$$PFD_{avg} = \frac{\beta \cdot \lambda_{du} \cdot T_{proof}}{2} + \lambda_{dd} \cdot MTTR + \frac{(1-\beta) \cdot \lambda_{du} \cdot LT}{2}\ , \qquad (1)$$

где β - эффективность теста по выявлению опасных отказов (принято 0,9);
λ_{du} - интенсивность необнаруженных опасных отказов;
T_{proof} - время между проведением проверочных диагностических тестов;
λ_{dd} - интенсивность обнаруженных опасных отказов;
MTTR – среднее время восстановления (8 ч);
LT – средний срок службы изделия (30 лет для исполнения атомное (повышенной надежности (средняя наработка на отказ – 270000 ч)); 15 лет для всех остальных исполнений (средняя наработка на отказ – 150000 ч)).

5 Запуск в эксплуатацию

5.1 Общее

Требуется выполнять рекомендации по монтажу и подключению, содержащиеся в руководстве по эксплуатации НКГЖ.406233.052РЭ.

6 Диагностика и обслуживание

Для связи с АИР-10SH, а также для проверки его настроек можно использовать любое HART-совместимое устройство.

Примечание – Выходной сигнал АИР-10SH не является безопасным в следующих случаях: при внесении изменений в конфигурацию, при проверке токовой петли 4 – 20 мА. Во время конфигурирования и технического обслуживания АИР-10SH необходимо применять альтернативные меры для обеспечения безопасности: либо дезактивировать функцию безопасности АИР-10SH (постановка АИР-10SH на байпас) для исключения ложного срабатывания системы безопасности, либо регламентные работы по обслуживанию АИР-10SH должны проводиться в остановочный ремонт.

Согласно разделу 7.4.5.2 f) ГОСТ Р МЭК 61508-2, для выявления опасных отказов, которые не могут быть определены диагностическими испытаниями, необходимо проводить контрольные испытания. Все работы, входящие в состав контрольных испытаний, должны проводиться квалифицированным персоналом.

В большинстве случаев, при проведении контрольного испытания, АИР-10SH должен быть либо поставлен на байпас – для исключения ложного срабатывания системы безопасности, либо регламентные работы по обслуживанию АИР-10SH должны проводиться в остановочный ремонт.

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"). Рекомендуемая форма протокола проверки приведена 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 контроля уровня рабочей среды на объекте.

Процедура № 2: устройство демонтировано, и есть возможность контроля уровня рабочей среды с помощью соответствующих испытательных устройств.

Для этого необходимо:

Подать давление, соответствующее 80 – 100% предела настройки АИР-10SH. Сбросить давление до начального и сравнить значение выходного сигнала АИР-10SH со значением, установленным при первичной настройке.

Ожидаемые результаты:

Выходной сигнал соответствует поданному давлению.

При выполнении контрольного испытания будут определены 50% опасных необнаруженных отказов.

ПРИЛОЖЕНИЕ А
Форма протокола 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 АИР-10SH
	Контроль параметров АИР-10SH на объекте
	Контрольная проверка с "подачей рабочей среды или демонтажом АИР-10SH"

Результат проверки		
Ожидаемое измеренное значение	Действительное значение	Результат проверки

Дата	Подпись

ПРИЛОЖЕНИЕ Б
Термины и 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 (далее – Э/Э/ЭП системы), связанных с безопасностью, и других средств по снижению риска.

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 (принимающий одно из четырёх значений), определяющий требования к полноте безопасности для функции безопасности, который ставится в соответствии с Э/Э/ПЭ системам, связанным с безопасностью.

Опасное состояние (dangerous state**)** - состояние процесса, при котором функция безопасности не может быть выполнена.

Безопасное состояние (safe state**)** – состояние процесса, в котором достигается безопасность. Функция безопасности выполнена.

Функция безопасности (safety function) – функция, реализуемая системой, связанной с безопасностью, основанной на других технологиях, или внешними средствами снижения риска, которая предназначена для достижения или поддержания безопасного состояния процесса применительно к определенному опасному событию.

Отказ (failure) – прекращение способности функциональной единицы выполнять требуемую функцию.

Опасный отказ (dangerous failure) – отказ, который потенциально может перевести систему, связанную с безопасностью, в опасное или неработоспособное состояние.

Безопасный отказ (safe failure) – отказ, который не переводит систему, связанную с безопасностью, в опасное состояние или в состояние отказа при выполнении функции.

Обнаруженный отказ (detected failure) – отказ, выявленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора (например, физического осмотра и ручной проверки) либо в ходе нормальной работы.

Необнаруженный отказ (undetected failure) – отказ, не выявленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора (например, физического осмотра и ручной проверки) либо в ходе нормальной работы.

Отказобезопасность – свойства изделия, ориентированные на сохранение безопасности в случае отказа.

Архитектура MooN – приборная система безопасности или ее часть, выполненная из N независимых каналов, соединеных так, что M каналов достаточно для выполнения функции безопасности.

FMEDA (Failure Modes, Effect, and Diagnostics Analysis) – анализ видов и последствий отказов, их эффектов и диагностики. Применяется для расчёта показателей функциональной безопасности.

Контрольная проверка/проверка функции безопасности (proof test) – периодическая проверка, выполняемая для того, чтобы обнаружить отказы в системе, связанной с безопасностью, с тем чтобы при необходимости система могла быть восстановлена настолько близко к исходному состоянию, насколько это возможно в данных условиях.

FIT (failures in time) – вероятность отказа, представляемая как число отказов на миллиард часов. 1 FIT = $1*10^{-9}$ в час.

DC (diagnostic coverage) – охват диагностикой, %.

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.

HFT (hardware fault tolerance) – допустимое число отказов оборудования.

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

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

PFH (average frequency of a dangerous failure per hour) - средняя частота опасного отказа в час, средняя частота опасного отказа Э/Э/ПЭ системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.