ПОВТОРИТЕЛИ СИГНАЛОВ ИСКРОБЕЗОПАСНЫЕ

ЛПА-310

Руководство по функциональной безопасности

Оглавление

1. Общие сведения....3
2. Сфера действия....3
2.1 Модификации устройства....3
2.2 Область применения....4
3. Проектирование....4
3.1 Режимы работы....4
3.2 Необходимые условия для правильной эксплуатации....4
3.3 Функция безопасности и безопасное состояние....6
4. Показатели функциональной безопасности....7
4.1 Показатели функциональной безопасности....7
4.2 Дополнительные сведения....7
5. Запуск в эксплуатацию....8
5.1 Общее....8
6. Диагностика и обслуживание....12
6.1 Контрольные проверки....12
6.2 Ремонт....13
Приложение А – Протокол проверки....14
Приложение Б – Определения....15

1. Общие сведения

Данное руководство по функциональной безопасности разработано в соответствии с ГОСТ Р МЭК 61508-2-2012 и действует для повторителей сигналов искробезопасных ЛПА-310 (в дальнейшем – повторителей).

Цель руководства по безопасности состоит в документальном оформлении информации, связанной с применяемыми повторителями сигналов искробезопасными ЛПА-310, 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 Модификации устройства

При заказе повторителей серии ЛПА-310 обозначение должно соответствовать виду ЛПА-310-XY0, где X — количество каналов, Y – наличие разветвления сигнала.

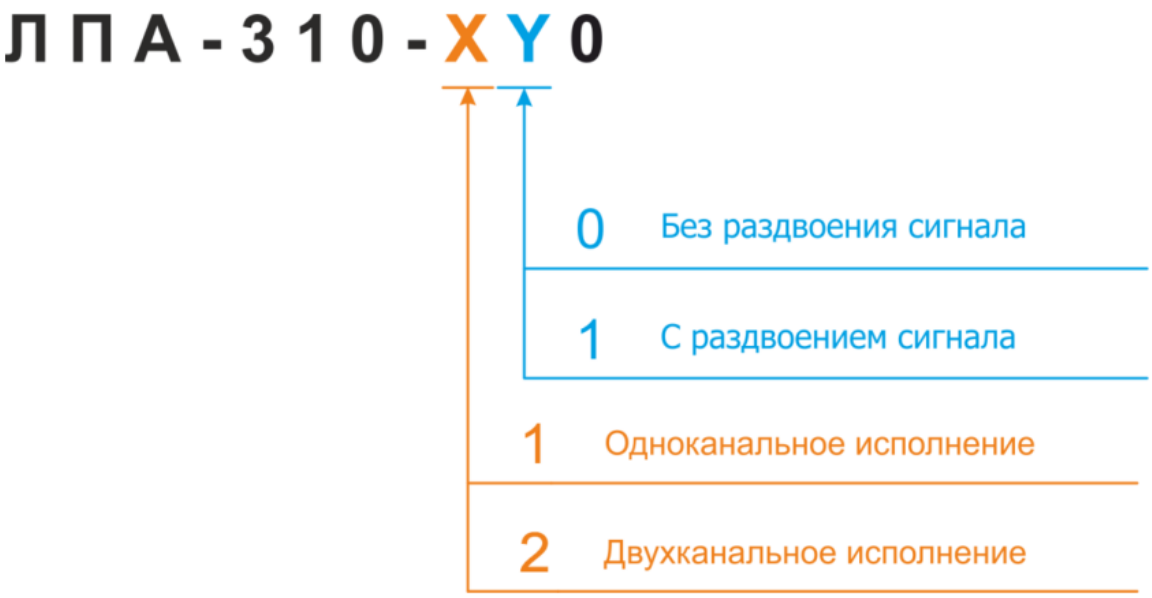


Рисунок 1. Обозначение повторителей

Функция разветвления сигнала доступна только для повторителя в одноканальном исполнении. Модификация ЛПА-310-210 к заказу не принимается. Выпускаемые модификации перечислены в таблице 1.

Таблица 1. Выпускаемые модификации повторителей

Модификация	Описание
ЛПА-310-100	Один канал
ЛПА-310-110	Один канал с раздвоением сигнала на 2 выхода
ЛПА-310-200	Два канала

2.2 Область применения

Повторители сигналов искробезопасные ЛПА-310 предназначены для обеспечения искробезопасности цепей взрывозащищенных первичных преобразователей, устанавливаемых во взрывоопасных зонах помещений и наружных установок, для обеспечения питания этих преобразователей, а также для линейного преобразования силы постоянного тока на входе повторителей в значения силы постоянного тока на его выходе при гальванической развязке электрических измерительных цепей.

Все повторители являются связанным оборудованием с искробезопасными входными цепями уровня «ia» по ГОСТ 31610.11-2014, имеют маркировку «[Ex ia Ma] I, [Ex ia Ga] IIC/IIB, [Ex ia Da] IIIC» и предназначены для установки вне взрывоопасных зон помещений и наружных установок.

К повторителям со стороны искробезопасных цепей могут подключаться устанавливаемые во взрывоопасных зонах помещений и наружных установок первичные преобразователи, имеющие сертификат соответствия ТР ТС 012/2011, выполненные с видом взрывозащиты «искробезопасная электрическая цепь i», маркировка взрывозащиты которых и максимальные значения параметров искробезопасных электрических цепей соответствуют маркировкам и максимальным значениям повторителей.

Повторители могут подключаться к вторичной аппаратуре, не имеющей гальванической развязки от регистрирующих устройств, но питаемой от силового трансформатора общего назначения.

Повторители рассчитаны на работу с унифицированным сигналом 4...20 мА постоянного тока. Повторители обеспечивают питание первичного измерительного преобразователя напряжением не менее 15 В при токе 20 мА. Повторители подключаются к первичному измерительному преобразователю по двухпроводной линии связи.

Повторители обеспечивают питание вторичного измерительного преобразователя напряжением 15 В ±5 %. Повторители подключаются к вторичному измерительному преобразователю по двухпроводной линии связи.

Подробные технические характеристики повторителей изложены в руководстве по эксплуатации ОЛПА-21.018.28 РЭ «Повторители сигналов искробезопасные ЛПА-310».

3. Проектирование

3.1 Режимы работы

Повторители могут применяться в связанных с безопасностью системах, в соответствии с ГОСТ Р МЭК 61508, в следующих режимах работы:

- режим с низкой частотой запросов (low demand mode), в котором функция безопасности выполняется только по запросу и переводит управляемое оборудование в определенное безопасное состояние, а частота запросов не превышает одного в год;
- режим с высокой частотой запросов (high demand mode), в котором функция безопасности выполняется только по запросу и переводит управляемое оборудование в определенное безопасное состояние, а частота запросов превышает один в год.

3.2 Необходимые условия для правильной эксплуатации

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

- Для двухканального исполнения ЛПА-310-200 только 1 канал может быть частью функции безопасности;
- 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;
- Устройства не защищены от сбоев электропитания. В обязанности пользователя входит обеспечение обнаружения низкого напряжения питания повторителя и адекватной реакции на эту неисправность;
- Повторители отнесены к типу А с отказоустойчивостью аппаратных средств HFT=0;
- Среднее время ремонта MTTR преобразователей составляет 8 часов;
- На время ремонта повторителя принимаются необходимые меры для сохранения функции безопасности (например, с помощью запасного повторителя);
- Протокол HART используется только для настройки, калибровки и диагностики первичных измерительных преобразователей, но не в процессе выполнения функции безопасности;
- Должны выдерживаться границы условий эксплуатации, указанные в руководстве по эксплуатации ОЛПА-21.018.28 РЭ «Повторители сигналов искробезопасные ЛПА-310»;
- Приведенные интенсивности отказов соответствуют рабочему диапазону температур -40…+70°С и относительной влажности до 90 % при 35 °С и более низких температурах без конденсации влаги при средней температуре за длительный период времени 40˚С. В случае более высокой средней температуры 60˚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;
- Рабочий диапазон преобразования постоянного тока от 4 до 20 мА;
- Система ПАЗ способна обнаруживать выход сигнала за пределы рабочего диапазона согласно стандарту NAMUR NE43;
- Все составные части измерительной цепи должны соответствовать предусмотренному уровню полноты безопасности "Safety Integrity Level (SIL)".

SIL2

- В режиме с низкой частотой запросов общее значение PFD_{avg} должно быть в диапазоне от 10^{-3} до 10^{-2};
- В режиме с высокой частотой запросов общее значение PFH должно быть в диапазоне от 10^{-7} до 10^{-6};
- Поскольку отказоустойчивость аппаратных средств равна 0 и повторитель является компонентом типа А, доля безопасных отказов компонентов SFF должна быть больше 60% в соответствии с таблицей 2 стандарта ГОСТ Р МЭК 61508-2-2012 для системы SIL2.

SIL3

SIL3 может быть достигнуть при использовании модификации ЛПА-310-110, если оба выхода подключены к одному ПЛК и разница в показаниях составляет менее 2%.

- В режиме с низкой частотой запросов общее значение PFD_{avg} должно быть в диапазоне от 10^{-4} до 10^{-3};
- В режиме с высокой частотой запросов общее значение PFH должно быть в диапазоне от 10^{-8} до 10^{-7};
- Поскольку отказоустойчивость аппаратных средств равна 0 и повторитель является компонентом типа А, доля безопасных отказов компонентов SFF должна быть больше 90% в соответствии с таблицей 2 стандарта ГОСТ Р МЭК 61508-2-2012 для системы SIL3.

При использовании преобразователей в многоканальной архитектуре требуется дополнительный расчёт показателей функциональной безопасности при пересчете на конкретный объект управления с другими аппаратными и программными средствами.

3.3 Функция безопасности и безопасное состояние

Функцией безопасности является повторение действующего значения входного аналогового сигнала 4…20 мА в выходной аналоговый сигнал 4…20 мА с точностью не хуже 2% за время не более 20 мс.

Со стороны взрывоопасной зоны к повторителю должен подключаться двухпроводный пассивный первичный преобразователь, эквивалентное входное сопротивление которого составляет не более 600 Ом.

Со стороны взрывобезопасной зоны к повторителю должен подключаться двухпроводный пассивный вторичный преобразователь, эквивалентное входное сопротивление которого составляет не более 600 Ом.

Для двухканального исполнения ЛПА-310-200 только 1 канал может быть частью функции безопасности (рис. 2а и 2б).

Разветвитель ЛПА-310-110 можно использовать в двух вариантах:

а) в функции безопасности используется только один выход (рис. 5а и 5б);

б) в функции безопасности используются оба выхода, при этой оба выхода подключены к одной системе ПАЗ (рис. 4).

Безопасное состояние: программа программируемого логического контроллера должна обнаруживать выход сигнала за пределы рабочего диапазона согласно стандарту NAMUR NE43 (<3,6 мА и >21 мА).

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 2. Показатели безопасности

Показатель	**ЛПА-310-200**	**ЛПА-310-100**	**ЛПА-310-110 1 выход (1oo1)**	**ЛПА-310-110 2 выхода (1oo2)**
Схема подключения	Рисунок 2	Рисунок 3	Рисунок 5	Рисунок 4
Уровень полноты безопасности (Safety Integrity Level)	**SIL2**	**SIL2**	**SIL2**	**SIL3**
Устойчивость к отказам аппаратных средств	HFT = 0			
Тип устройства	Тип А			
Режим работы	С низкой частотой запросов, с высокой частотой запросов			
SFF	70,32	70,25	81,80	92,24
λ_{DU}	171 FIT	171 FIT	182 FIT	84,6 FIT
λ_{DD}	405 FIT	403 FIT	818 FIT	898 FIT
λ_{SD}	0	0	0	107 FIT
λ_{SU}	0	0	0	1,08 FIT
PFH*	$1{,}71\cdot10^{-7}$	$1{,}71\cdot10^{-7}$	$1{,}82\cdot10^{-7}$	$8{,}5\cdot10^{-9}$
PFD_{avg} (T_{proof} = 1 год)	$7{,}53\cdot10^{-4}$	$7{,}53\cdot10^{-4}$	$8{,}05\cdot10^{-4}$	$3{,}77\cdot10^{-5}$
PFD_{avg} (T_{proof} = 2 года)	$1{,}5\cdot10^{-3}$	$1{,}5\cdot10^{-3}$	$1{,}6\cdot10^{-3}$	$7{,}55\cdot10^{-5}$
PFD_{avg} (T_{proof} = 3 года)	$2{,}25\cdot10^{-3}$	$2{,}25\cdot10^{-3}$	$2{,}40\cdot10^{-3}$	$1{,}14\cdot10^{-4}$
PFD_{avg} (T_{proof} = 5 лет)	$3{,}75\cdot10^{-3}$	$3{,}75\cdot10^{-3}$	$3{,}99\cdot10^{-3}$	$1{,}92\cdot10^{-4}$
PFD_{avg} (T_{proof} = 10 лет)	$7{,}49\cdot10^{-3}$	$7{,}49\cdot10^{-3}$	$7{,}98\cdot10^{-3}$	$3{,}96\cdot10^{-4}$
Средняя наработка до отказа (MTTF)**, ч	552 861	1 079 985	575 203	
Среднее время восстановления (MTTR), ч	8			
Средняя наработка между отказами (MTBF), ч	552 869	1 079 993	575 211	

* Зеленым цветом выделены значения PFH и PFDavg, которые занимают ≤10% от общего количества опасных отказов для SIL2 (SIL3) контура безопасности. Желтым цветом выделены значения PFH и PFDavg, которые занимают >10% от общего количества опасных отказов для SIL2 (SIL3) контура безопасности.

** Значение средней наработки до отказа включает в себя значения интенсивностей отказов компонентов, не являющихся частью функции 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 1oo1 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 1oo2 были рассчитаны следующим образом:

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

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

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

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

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 1oo1, 1oo2, 2oo2 и 2oo3;

t_{GE} – эквивалентное среднее время простоя голосующей группы для архитектур 1oo1, 1oo2, 2oo2 и 2oo3;

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;

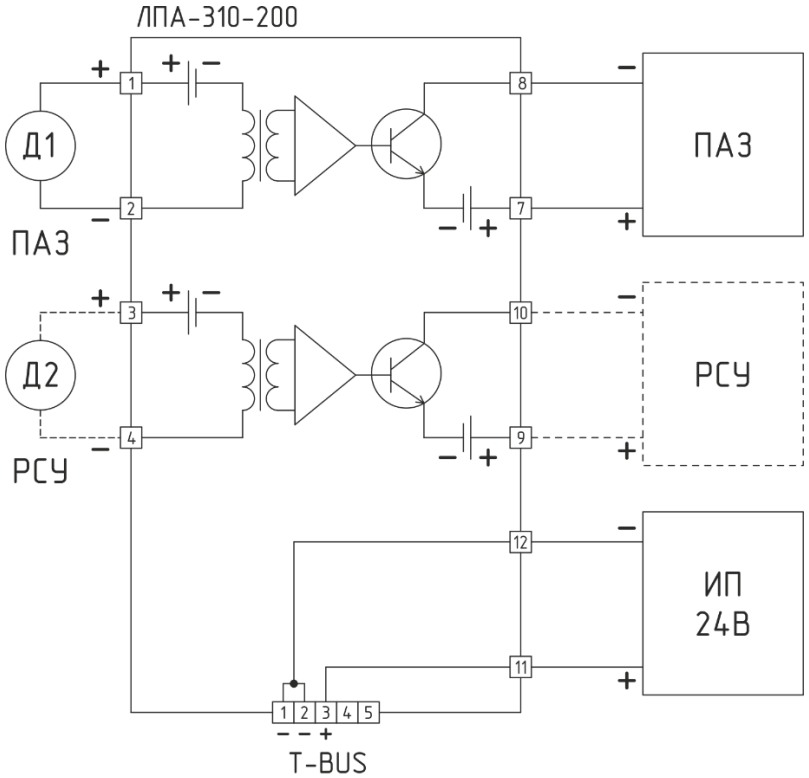
MRT – средняя продолжительность нахождения устройства в неработоспособном состоянии, обусловленном его ремонтом, принято 8ч.

5. Запуск в эксплуатацию

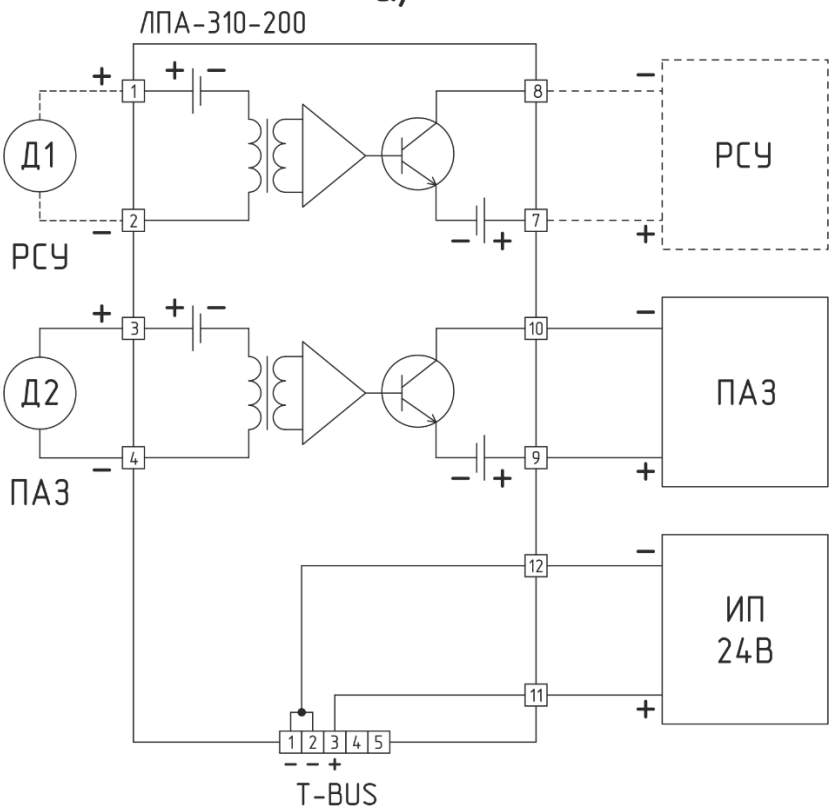
5.1 Общее

Требуется выполнять содержащиеся в руководстве по эксплуатации ОЛПА-21.018.28 РЭ «Повторители сигналов искробезопасные ЛПА-310» рекомендации по монтажу и подключению преобразователя.

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



а)



б)

Рисунок 2. Схема подключения к повторителю ЛПА-310-200

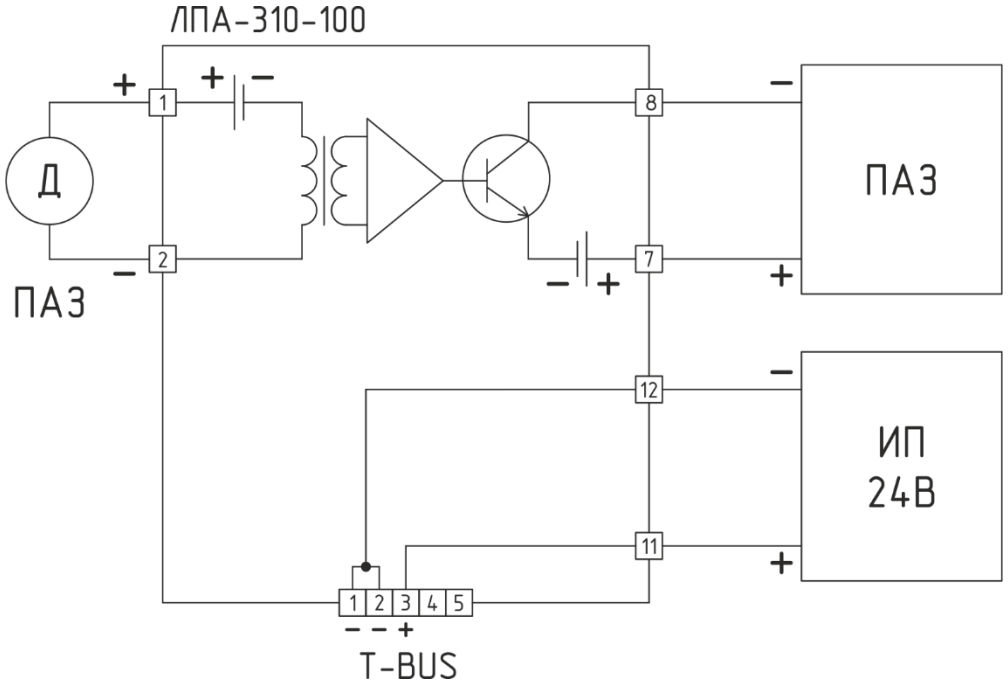


Рисунок 3. Схема подключения к повторителю ЛПА-310-100

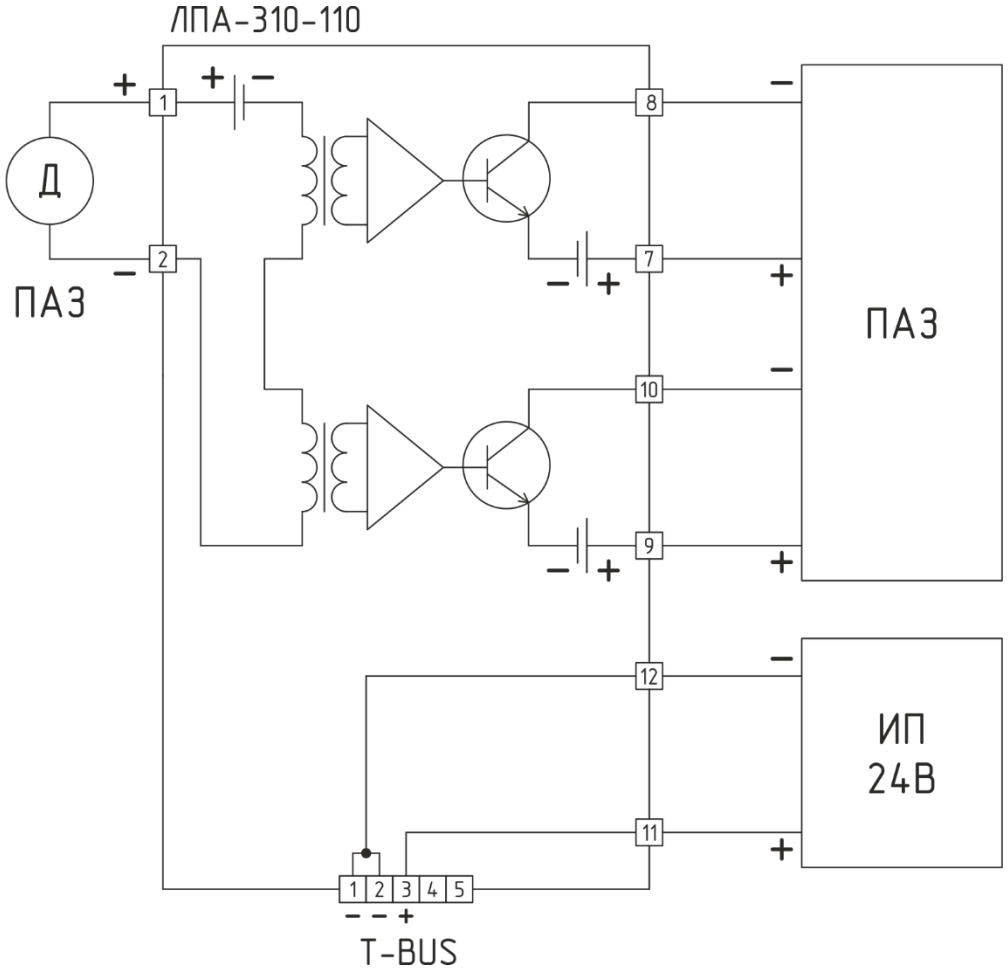


Рисунок 4. Схема подключения к повторителю ЛПА-310-110 с использованием в функции безопасности обоих выходов (1оо2)

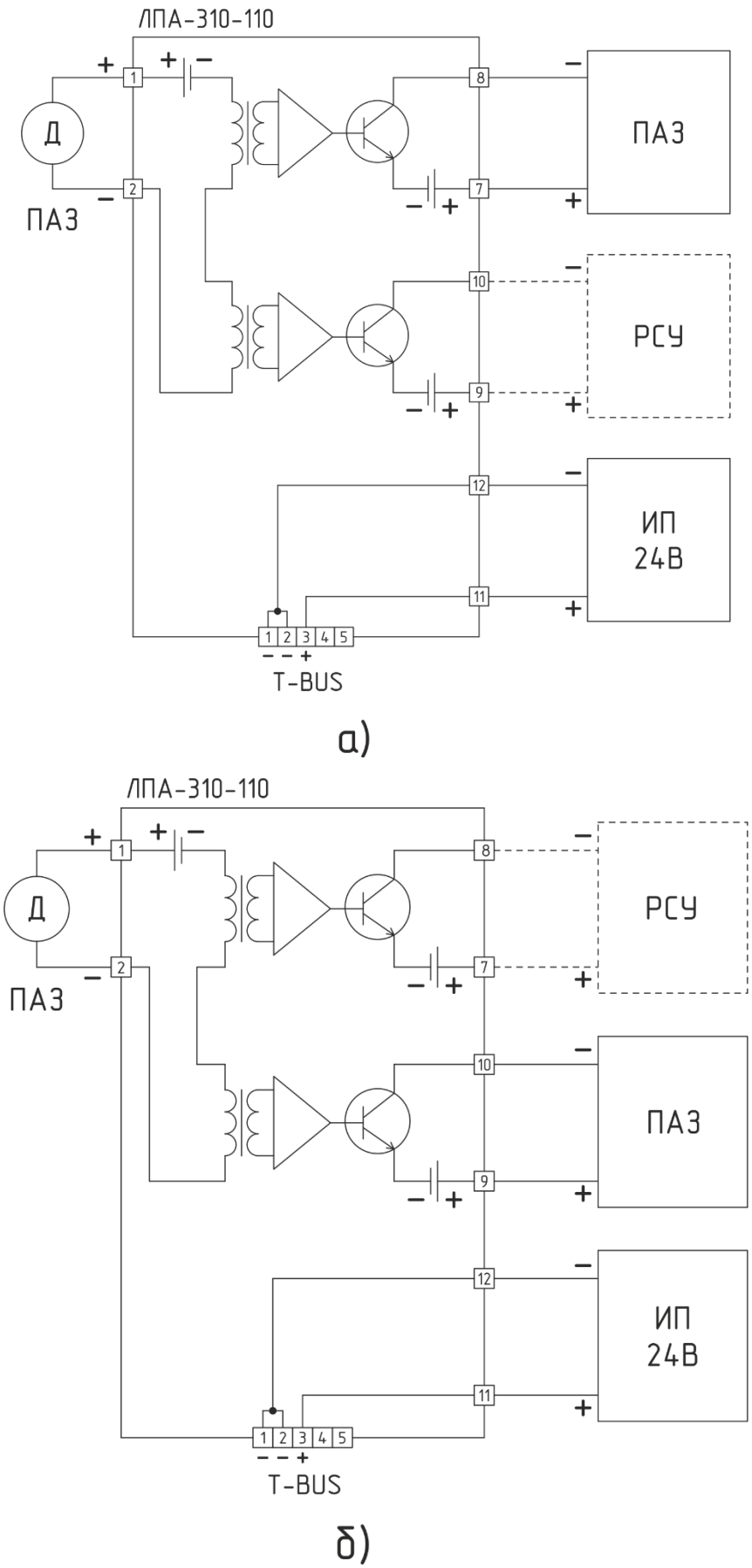


Рисунок 5. Схема подключения к повторителю ЛПА-310-110 с использованием в функции безопасности только одного выхода (1oo1)

Допускается для выполнения функции безопасности использовать повторители ЛПА-310 с объединительными модулями ЛПА-300. Подробную информацию об объединительных модулях можно найти в ОЛПА-31.013.01 РЭ «Объединительные модули ЛПА-300».

6. Диагностика и обслуживание

6.1 Контрольные проверки

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.

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 контрольной проверки необходимо

Последовательно подать значения входного сигнала согласно таблице 3. Измерить значения выходного сигнала. Справочные значения входного сигнала и допустимые значения выходного сигнала приведены в таблице 3.

Таблица 3. Данные для контрольной проверки

Iвх, мА	Допускаемые значения Iвых, мА	
	мин.	макс.
4,000	3,680	4,320
8,000	7,680	8,320

12,000	11,680	12,320
16,000	15,680	16,320
20,000	19,680	20,320

Ожидаемые результаты:

Значения выходного сигнала повторителя соответствуют поданным значениям входного сигнала.

Охват проверки

Остающиеся опасные необнаруженные ошибки составляют 85-182 FIT (охват диагностики 95%).

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.

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 повторителя
	Контроль параметров повторителя на объекте
	Контрольная проверка с демонтажом повторителя

Iкал, мА	Iвых, мА	γ, %	Допускаемые значения Iвых, мА	
			мин.	макс.
4,000			3,680	4,320
8,000			7,680	8,320
12,000			11,680	12,320
16,000			15,680	16,320
20,000			19,680	20,320

Дата:	Подпись:

Приложение Б – 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.

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

ПАЗ – противоаварийная защита.

РСУ – распределенная система управления.

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 (принимающий 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.