БАРЬЕРЫ ИСКРОБЕЗОПАСНОСТИ ЛПА-340

Руководство по функциональной безопасности

Версия 3

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 5
3.3 Входные сигналы, выходные сигналы, функция безопасности и безопасное состояние 7
3.3.1 Входные сигналы 7
3.3.2 Выходные сигналы 7
3.3.3 Функция безопасности и безопасное состояние выходных цепей 7
4. Показатели функциональной безопасности 10
4.1 Показатели функциональной безопасности 10
4.2 Дополнительные сведения 11
5. Запуск в эксплуатацию 12
5.1 Общее 12
5.2 Конфигурирование барьеров 12
5.3 Схемы подключения 13
6. Диагностика и обслуживание 18
6.1 Контрольные проверки 18
6.2 Состав контрольных проверок 19
6.3 Ремонт 19
Приложение А – Протокол проверки 20
Приложение Б – Определения 21

1. Общие сведения

Настоящее руководство по функциональной безопасности (далее – РФБ) разработано в соответствии с **ГОСТ Р МЭК 61508-2-2012** и действует для барьеров искробезопасности ЛПА-340-100 и ЛПА-340-220 (в дальнейшем – барьеров).

Цель РФБ состоит в документальном оформлении информации, связанной с применяемыми барьерами, 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

Данное РФБ распространяется на модификации ЛПА-340-100 и ЛПА-340-220.

Таблица 1. Основные характеристики барьеров

Сравнительная характеристика	**ЛПА-340-100**	**ЛПА-340-220**
Количество каналов	1	2
Максимальная частота переключения	10 Гц	
Встроенная диагностика	- контроль целостности цепей подключения датчика - контроль внутреннего источника питания барьера	
Блокировка диагностики	Да	
Разветвление сигнала	Нет	Есть
Инверсия выходных сигналов	Есть	
Тип выходного сигнала	Оптореле	NAMUR EN 60947-5-6 (ГОСТ IEC 60947-5-6-2017)
Нагрузочная способность выхода	30 В, 300 мА постоянного или переменного тока	NAMUR EN 60947-5-6 (ГОСТ IEC 60947-5-6-2017)

2.2 Область применения

Барьеры ЛПА-340-100 и ЛПА-340-220 предназначены для обеспечения искробезопасности цепей подключения дискретных датчиков стандарта **NAMUR EN 60947-5-6 (ГОСТ IEC 60947-5-6-2017)**, далее – **NAMUR**, датчиков типа «сухой контакт» с контролем целостности цепи, «сухой контакт» без контроля целостности цепи, устанавливаемых во взрывоопасных зонах помещений и наружных установок. Барьеры обеспечивают искробезопасное питание и контроль целостности цепей подключения дискретных датчиков, прием дискретных сигналов от датчиков, воспроизведение сигналов датчиков и состояния цепей их подключения на своем выходе (со стороны взрывобезопасной зоны) в различных форматах, соответствующую светодиодную индикацию с одновременным обеспечением гальванической развязки между цепями подключения датчиков, выходными цепями и цепями питания барьера.

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

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

Барьеры подключаются к первичному измерительному преобразователю по двухпроводной линии связи.

Подробные технические характеристики барьеров изложены в руководстве по эксплуатации ОЛПА-21.018.29 РЭ «Барьеры искробезопасности ЛПА-340» (далее – РЭ).

3. Проектирование

3.1 Режимы работы

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

- **Режим с низкой частотой запросов (low demand mode):** режим, 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 или непрерывный режим (high demand mode):** режим, 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 были приняты следующие допущения:

- Барьеры относятся к типу **A** с отказоустойчивостью **HFT**=0;
- 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;
- Приведенные интенсивности отказов соответствуют рабочему диапазону температур -40…+70°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;
- В случае возникновения безопасного отказа (например, в случае перехода выхода барьера в безопасное состояние), среднее время восстановления (ремонта) барьеров (**MTTR**) составляет 8 часов (например, восстановление цепей подключения датчика);
- На время ремонта барьера, проведения диагностического тестирования и т. п. принимаются необходимые меры для сохранения функции безопасности (например, с помощью запасного барьера);
- Все составные части измерительной цепи должны соответствовать предусмотренному уровню полноты безопасности "Safety Integrity Level (SIL)";
- Устройства не защищены от сбоев электропитания. В обязанности пользователя входит обеспечение обнаружения низкого напряжения питания повторителя и адекватной реакции на эту неисправность;
- Отказы, произошедшие вследствие конфигурирования барьеров в процессе работы - не рассматриваются. Все настройки и конфигурирование должны быть произведены в соответствие с требованиями настоящего РФБ и РЭ до ввода в эксплуатацию;
- Все барьеры могут работать в режимах с низкой и высокой частотой запросов;
- Система ПАЗ должна быть способна принимать и обрабатывать сигналы согласно стандарту **NAMUR** (для работы с ЛПА-340-220), включая детектирование состояний «неисправность», либо поддерживать работу с дискретными сигналами с контролем цепей КЗ и Обрыв (для работы с ЛПА-340-100 с контролем цепей подключения барьера к системе ПАЗ);
- Для ЛПА-340-220 только 1 канал может быть частью функции безопасности. Допускаются к применению в составе функции, связанной с безопасностью, только описанные в настоящем РФБ конфигурации выходных сигналов барьеров;
- Функция контроля целостности цепей подключения датчика на барьерах должна быть активирована;

- Любые неиспользуемые входы и выходы не должны иметь никаких внешних подключений;
- Опторелейные выходы ЛПА-340-100 должны быть нагружены не более, чем на 240 мА по току и 24 В по напряжению (80% от предельной нагрузочной способности, указанной в РЭ), и защищены предохранителями соответствующего номинала.
- Должны выдерживаться границы условий эксплуатации, указанные в РЭ, если не оговорено иное.

SIL2

- Доля безопасных отказов барьера для контура безопасности с уровнем полноты безопасности **SIL2** не должна превышать 10% от полной величины;
- Для систем, связанных с безопасностью, с уровнем полноты безопасности **SIL2**, работающих в режиме с низкой частотой запросов, полное значение **PFDavg** для функции безопасности (**SIF**) гарантированно не должно превышать 10^{-2};
- Для систем, связанных с безопасностью с уровнем полноты безопасности **SIL2**, работающих в режиме с высокой частотой запросов, полное значение **PFH** для функции безопасности (**SIF**) гарантированно не должно превышать 10^{-6} в час;
- Для устройств типа типу **A** с отказоустойчивостью **HFT**=0, значение **SFF** должно быть не менее 60 %, в соответствие с таблицей 2 стандарта **МЭК 61508-2** для подсистем с уровнем полноты безопасности **SIL2**.

SIL3

- Доля безопасных отказов барьера для контура безопасности с уровнем полноты безопасности **SIL3** не должна превышать 10% от полной величины;
- Для систем, связанных с безопасностью, с уровнем полноты безопасности **SIL3**, работающих в режиме с низкой частотой запросов, полное значение **PFDavg** для функции безопасности (**SIF**) гарантированно не должно превышать 10^{-3};
- Для систем, связанных с безопасностью с уровнем полноты безопасности **SIL3**, работающих в режиме с высокой частотой запросов, полное значение **PFH** для функции безопасности (**SIF**) гарантированно не должно превышать 10^{-7} в час;
- Для устройств типа типу **A** с отказоустойчивостью **HFT**=0, значение **SFF** должно быть не менее 90 %, в соответствие с таблицей 2 стандарта **МЭК 61508-2** для подсистем с уровнем полноты безопасности **SIL3**.

3.3 Входные сигналы, выходные сигналы, функция безопасности и безопасное состояние

3.3.1 Входные сигналы

В применениях, связанных с безопасностью, со стороны взрывоопасной зоны к барьерам ЛПА-340-100 и ЛПА-340-220, должны подключаться:
- двухпроводные датчики, соответствующие стандарту **NAMUR**;
- двухпроводные датчики типа «сухой контакт» с оконечными элементами.

На Рисунок 1 приведен пример использования резисторов в качестве оконечных элементов для реализации функции контроля цепей подключения датчика типа «сухой контакт». Оконечные резисторы должны быть установлены как можно ближе к контактной группе датчика, номинал резистора R1 следует принять равным 20 кОм ± 10%, номинал резистора R2 – 2 кОм ± 10%, номинальная мощность резисторов должна быть не менее 0,1 Вт.

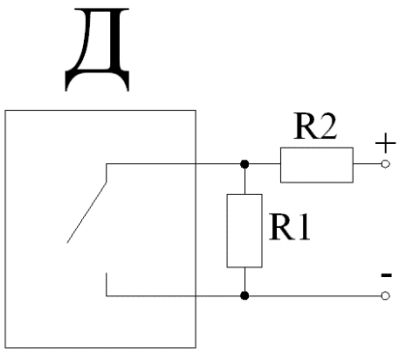

Рисунок 1. Схема обвязки дискретного датчика с поддержкой контроля цепи

В системах, связанных с безопасностью, не допускается применение датчиков типа «сухой контакт» без оконечных элементов!

3.3.2 Выходные сигналы

Выходные сигналы барьеров ЛПА-340-100 выполнены в формате оптореле, которые могут находиться в двух состояниях (разомкнуто или замкнуто).

Выходные сигналы барьеров ЛПА-340-220 выполнены в формате **NAMUR** и поддерживают четыре состояния (разомкнут, замкнут, обрыв, короткое замыкание).

3.3.3 Функция безопасности и безопасное состояние выходных цепей

Функция безопасности барьера состоит в корректном транслировании состояния входного состояния датчика на свой выход за время, не более 20 мс, и непосредственно связана с безопасным состоянием выходных сигнальных цепей. Предусмотрено два режима работы: прямой (без инверсии полезного сигнала) и инверсный (с инверсией полезного сигнала).

Безопасным состоянием выходов барьера ЛПА-340-100 является любая комбинация состояний выходов «Выход 1» и «Ошибка 1», когда хотя бы один из них находится в разомкнутом состоянии, т. е. питание с одного или обоих оптореле снято. Безопасное

состояние выходов барьера ЛПА-340-100, зависимость их состояния от входного сигнала, а также состояние индикации барьера в зависимости от его конфигурации приведены в Таблица 2 (ячейки, соответствующие безопасному состоянию выходных цепей, выделены жирным шрифтом и цветом).

Таблица 2 Безопасное состояние выходных цепей и индикация ЛПА-340-100 для первого канала, включенного в систему ПАЗ

«Вход 1»	Ток датчика, мА	Инверсия Выход 1 (DIP4)	«Выход 1»	«Ошибка 1»	Индикация «Питание»	Индикация «Канал 1»*
ИБ питание в норме: линия связи исправна, датчик включен	2,1 ≤ Iд ≤ 6,4	OFF	Замкнут	Замкнут	Зеленый	Зеленый
		ON	***Разомкнут***		Зеленый	Зеленый
ИБ питание в норме: линия связи исправна, датчик выключен	0,4 ≤ Iд ≤ 1,2	OFF	***Разомкнут***	Замкнут	Зеленый	Не горит
		ON	Замкнут		Зеленый	Не горит
ИБ питание в норме: КЗ линии связи	Iд ≥ 6,5	OFF	Замкнут	***Разомкнут***	Зеленый	Зеленый+ Красный
		ON	***Разомкнут***		Зеленый	Зеленый+ Красный
ИБ питание в норме: обрыв линии связи	Iд ≤ 0,2	OFF	***Разомкнут***	***Разомкнут***	Зеленый	Красный
		ON	Замкнут		Зеленый	Красный
Неисправность ИБ питания: датчик включен или КЗ линии связи	Iд ≥ 2,1	OFF	Замкнут	***Разомкнут***	Красный	Зеленый+ Красный
		ON	***Разомкнут***		Красный	Зеленый+ Красный
Неисправность ИБ питания: датчик выключен или обрыв линии связи	Iд ≤ 1,2	OFF	***Разомкнут***	***Разомкнут***	Красный	Красный
		ON	Замкнут		Красный	Красный

* - ***индикация отображает состояние входных цепей.***

Безопасным состоянием выходов барьера ЛПА-340-220 является либо состояние «Деактивирован» (высокоимпедансное состояние, в терминах стандарта **NAMUR**), либо любое состояние «Неисправность» (реализуется при возникновении обрыва, короткого замыкания линии связи с датчиком или любой диагностированной внутренней неисправности барьера). Безопасное состояние выходов барьера ЛПА-340-220, зависимость их состояния от входного сигнала, а также состояние индикации барьера в зависимости от его конфигурации приведены в Таблица 3 (ячейки, соответствующие безопасному состоянию выходных цепей, выделены жирным шрифтом и цветом).

Таблица 3 Безопасное состояние выходных цепей и индикация ЛПА-340-220 для первого канала, включенного в систему ПАЗ

«Вход 1»	Ток датчика, мА	Инверсия Выход 1 (DIP4)	«Выход 1»*	Индикация «Питание»	Индикация «Канал 1»**
ИБ питание в норме: линия связи исправна, датчик включен	2,1 ≤ Iд ≤ 6,4	OFF	3 ≤ Iвых ≤ 5	Зеленый	Зеленый
		ON	***0,5 ≤ Iвых ≤ 1,1***	Зеленый	Зеленый
ИБ питание в норме: линия связи исправна, датчик выключен	0,4 ≤ Iд ≤ 1,2	OFF	***0,5 ≤ Iвых ≤ 1,1***	Зеленый	Не горит
		ON	3 ≤ Iвых ≤ 5	Зеленый	Не горит
ИБ питание в норме: КЗ линии связи	Iд ≥ 6,5	OFF	***Iвых ≥ 7,2***	Зеленый	Зеленый+ Красный
		ON	***Iвых ≥ 7,2***	Зеленый	Зеленый+ Красный
ИБ питание в норме: обрыв линии связи	Iд ≤ 0,2	OFF	***Iвых ≤ 0,2***	Зеленый	Красный
		ON	***Iвых ≤ 0,2***	Зеленый	Красный
Неисправность ИБ питания: датчик включен или КЗ линии связи	Iд ≥ 2,1	OFF	***Iвых ≥ 7,2***	Красный	Зеленый+ Красный
		ON	***Iвых ≥ 7,2***	Красный	Зеленый+ Красный
Неисправность ИБ питания: датчик выключен или обрыв линии связи	Iд ≤ 1,2	OFF	***Iвых ≤ 0,2***	Красный	Красный
		ON	***Iвых ≤ 0,2***	Красный	Красный

* - ***указанные величины выходных токов барьеров ЛПА-340-220 даны с учетом подключения к тестовой схеме, описанной в разделе 9.2 стандарта NAMUR;***

** - ***индикация отображает состояние входных цепей.***

4. Показатели функциональной безопасности

4.1 Показатели функциональной безопасности

Таблица 4. Показатели безопасности

Показатель	**ЛПА-340-100**									**ЛПА-340-220**	
Схема подключения	Рис. 2,3			Рис. 4			Рис. 5,6			Рис. 7,8,9	
Режим работы (положение DIP-переключателей)*	0000000		0001000	0000000		0001000	0000000		0001000	**X0X0X**00	**X0X1X**00
Уровень полноты безопасности	SIL2	SIL3	SIL2	SIL2	SIL3	SIL2	SIL2	SIL3	SIL2	SIL2	
Устойчивость к отказам аппаратных средств	HFT = 0										
Тип устройства	Тип А										
Режим работы	С низкой частотой запросов, с высокой частотой запросов										
SFF, %	92,19		83,67	92,19		83,67	92,13		83,44	87,02	79,98
$\lambda_{du\ (FIT)}$	32,80		68,65	32,80		68,65	33,06		69,59	66,04	101,85
$\lambda_{dd\ (FIT)}$	0,00		0,00	0,00		0,00	26,06		93,83	0,00	0,00
$\lambda_{sd\ (FIT)}$	0,00		0,00	316,11		316,44	290,05		222,61	373,37	373,70
$\lambda_{su\ (FIT)}$	387,37		351,70	71,26		35,26	70,99		34,31	69,25	33,29
PFH**	3,28E-08	3,28E-08	6,86E-08	3,28E-08	3,28E-08	6,86E-08	3,31E-08	3,31E-08	6,96E-08	6,60E-08	1,02E-07
PFD_{avg} (T_{proof} = 1 год)**	1,44E-04	1,44E-04	3,01E-04	1,44E-04	1,44E-04	3,01E-04	1,45E-04	1,45E-04	3,06E-04	2,90E-04	4,47E-04
PFD_{avg} (T_{proof} = 2 года)**	2,88E-04	2,88E-04	6,02E-04	2,88E-04	2,88E-04	6,02E-04	2,90E-04	2,90E-04	6,11E-04	5,79E-04	8,93E-04
PFD_{avg} (T_{proof} = 3 года)**	4,31E-04	4,31E-04	9,03E-04	4,31E-04	4,31E-04	9,03E-04	4,35E-04	4,35E-04	9,16E-04	8,68E-04	1,34E-03
PFD_{avg} (T_{proof} = 5 лет)**	7,19E-04	7,19E-04	1,50E-03	7,19E-04	7,19E-04	1,50E-03	7,25E-04	7,25E-04	1,53E-03	1,45E-03	2,23E-03
PFD_{avg} (T_{proof} = 10 лет)**	1,44E-03	-	3,01E-03	1,44E-03	-	3,01E-03	1,45E-03	-	3,05E-03	2,89E-03	4,46E-03
Средняя наработка до отказа (MTTF), ч***	1387727									890995	
Среднее время восстановления (MTTR), ч	8										
Средняя наработка между отказами (MTBF), ч	1387735									891003	

**** Символом "X" обозначены переключатели, положение которых может быть любым.***

***** Зеленым цветом выделены значения PFH и PFDavg изделия, которые занимают ≤10% от общего бюджета соответствующего показателя для контура безопасности в целом при заявленном уровне полноты безопасности (SIL2 или SIL3). Желтым цветом выделены значения PFH и PFDavg изделия, которые занимают >10% от общего бюджета соответствующего показателя для контура безопасности в целом при заявленном уровне полноты безопасности (SIL2 или SIL3).***

****** Значение средней наработки до отказа включает в себя значения интенсивностей отказов компонентов, не являющихся частью функции безопасности.***

4.2 Дополнительные сведения

Доля безопасных отказов показывает отношение общего количества всех безопасных и всех опасных диагностируемых отказов к общему числу отказов:

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

Доля безопасных отказов, в соответствии с **ГОСТ Р МЭК 61508**, относится только к элементам или подсистемам в полном контуре безопасности. Рассматриваемое устройство всегда является частью полного контура безопасности и не рассматривается как законченный элемент или подсистема. Для расчета **SIL** контура безопасности необходимо оценить долю безопасных отказов всех элементов, подсистем и системы в целом, а не только для отдельного устройства. Тем не менее, **SFF** устройства приведен в этом документе для справки.

Значения PFD_{AVG} для архитектуры 1oo1 были рассчитаны следующим образом:

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

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

t_{CE} – эквивалентное среднее время простоя канала для архитектур 1oo1;

λ_{DU} – интенсивность необнаруженных опасных отказов;

λ_{DD} – интенсивность обнаруженных опасных отказов;

λ_{SU} – интенсивность необнаруженных безопасных отказов;

λ_{SD} – интенсивность обнаруженных безопасных отказов;

$\lambda_D = \lambda_{DU} + \lambda_{DD}$;

Tproof – время между проведением проверочных диагностических тестов

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

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

5. Запуск в эксплуатацию

5.1 Общее

Необходимо выполнять содержащиеся в РЭ и настоящем РФБ требования и рекомендации по монтажу, конфигурированию и подключению барьеров.

Допускается для выполнения функции безопасности использовать барьеры ЛПА-340-100 и ЛПА-340-220 совместно с объединительными модулями ЛПА-300. Подробную информацию об объединительных модулях можно найти в ОЛПА-31.013.01 РЭ «Объединительные модули ЛПА-300».

5.2 Конфигурирование барьеров

Барьеры ЛПА-340-100 и ЛПА-340-220 предусматривают возможность конфигурирования режимов работы посредством DIP-переключателей. Допустимые режимы работы в системах ПАЗ перечислены в (см. Таблица 5).

Таблица 5 Режимы работы, допустимые к применению в системе ПАЗ

Модификация	**Режимы работы**						
	Разветвление	**Блокировка КЦ Вход 1**	**Блокировка КЦ Вход 2**	**Инверсия Выход 1**	**Инверсия Выход 2**	**Не используется**	
	DIP1	**DIP2**	**DIP3**	**DIP4**	**DIP5**	**DIP6**	**DIP7**
ЛПА-340-100	**OFF ***	**OFF ***	**OFF ***	OFF	**OFF ***	**OFF ***	**OFF ***
	OFF *	**OFF ***	**OFF ***	ON	**OFF ***	**OFF ***	**OFF ***
ЛПА-340-220	OFF	**OFF ***	OFF	OFF	OFF	**OFF ***	**OFF ***
	OFF	**OFF ***	OFF	OFF	ON	**OFF ***	**OFF ***
	OFF	**OFF ***	OFF	ON	OFF	**OFF ***	**OFF ***
	OFF	**OFF ***	OFF	ON	ON	**OFF ***	**OFF ***
	OFF	**OFF ***	ON	OFF	OFF	**OFF ***	**OFF ***
	OFF	**OFF ***	ON	OFF	ON	**OFF ***	**OFF ***
	OFF	**OFF ***	ON	ON	OFF	**OFF ***	**OFF ***
	OFF	**OFF ***	ON	ON	ON	**OFF ***	**OFF ***
	ON	**OFF ***	OFF	OFF	OFF	**OFF ***	**OFF ***
	ON	**OFF ***	OFF	OFF	ON	**OFF ***	**OFF ***
	ON	**OFF ***	OFF	ON	OFF	**OFF ***	**OFF ***
	ON	**OFF ***	OFF	ON	ON	**OFF ***	**OFF ***
	ON	**OFF ***	ON	OFF	OFF	**OFF ***	**OFF ***
	ON	**OFF ***	ON	OFF	ON	**OFF ***	**OFF ***
	ON	**OFF ***	ON	ON	OFF	**OFF ***	**OFF ***
	ON	**OFF ***	ON	ON	ON	**OFF ***	**OFF ***

**** - в системах, связанных с безопасностью, блокировка функции контроля цепей подключения датчика первого канала должна быть отключена (DIP2=OFF) для всех рассматриваемых модификаций барьеров, кроме прочего, все неиспользуемые переключатели также должны быть отключены (переведены в положение OFF): DIP1, DIP3, DIP5, DIP6, DIP7 - для ЛПА-340-100 и DIP6, DIP7 - для ЛПА-340-220.***

Все настройки и конфигурирование должны производиться до ввода в эксплуатацию, в строгом соответствии с требованиями настоящего РФБ и РЭ.

5.3 Схемы подключения

ЛПА-340-100 и ЛПА-340-220 реализуют аппаратную архитектуру 1001, когда сигнал ошибки барьера непосредственно участвует в формировании безопасного состояния выходных цепей. В случае ЛПА-340-100 это в явном виде может быть реализовано в шлейфовой топологии, объединяющей два размыкающихся контакта, либо раздельным приемом обоих сигналов и дальнейшей их логической обработкой в системе ПАЗ. При этом, сигнал «Выход 1» управляется входным сигналом канала и логика его работы может быть инвертирована (см. 3.3.3), а сигнал «Ошибка 1» всегда замкнут при отсутствии неисправностей. В случае ЛПА-340-220 это реализовано в самой структуре двухпроводного сигнала стандарта **NAMUR**, уже содержащего как информацию о полезном сигнале, так и диагностическую информацию. т. е. имеет 4 контролируемых состояния. Во всех случаях используется схема «один вход – один выход» (один канал барьера) в составе одного контура ПАЗ.

На всех схемах состояние контактов выходных сигналов показано для дежурного режима, когда отсутствуют неисправности и нет запроса на перевод выходных цепей барьера в безопасное состояние и выполнение функции безопасности (оба контакта замкнуты). Датчики изображены условно и не учитывают зависимость состояния выходов от состояния входного сигнала (зависит от статуса функции инверсии, см. Таблица 2 для ЛПА-340-100 и Таблица 3 для ЛПА-340-220).

Барьер ЛПА-340-100

На Рисунок 2 показан вариант подключения барьера ЛПА-340-100 к системе ПАЗ для работы в составе одного контура ПАЗ, прямо реализующий архитектуру 1001.

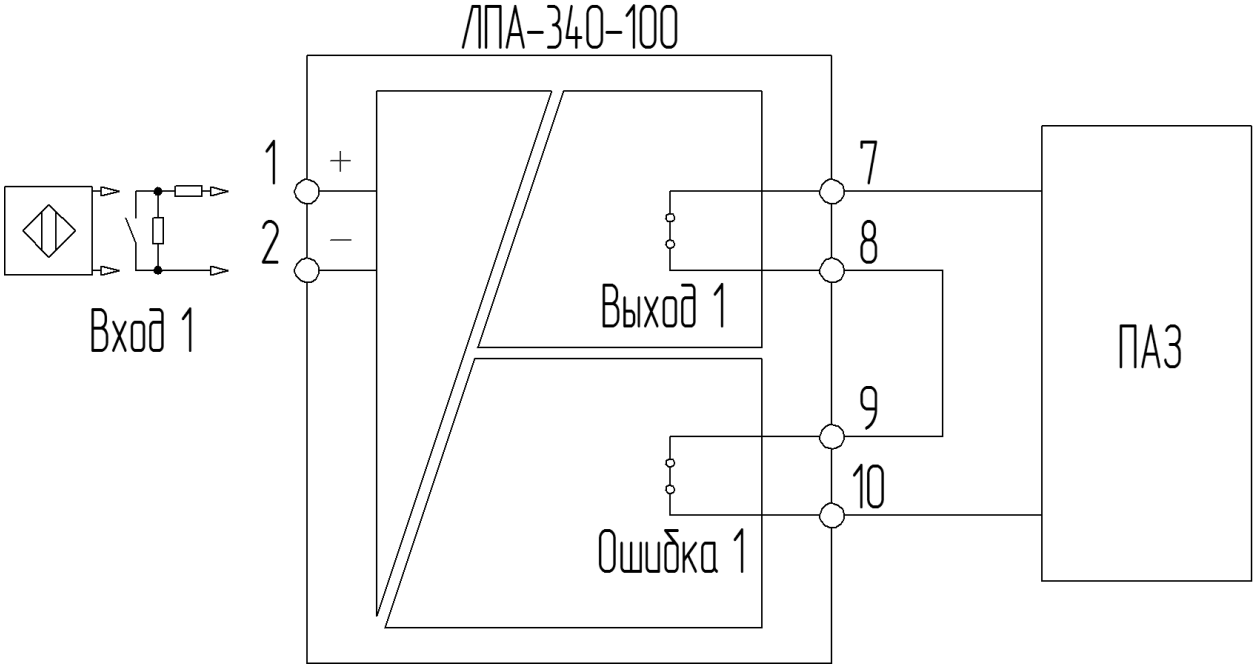

Рисунок 2 Подключение ЛПА-340-100 к системе ПАЗ единым шлейфом без контроля целостности

В данном варианте не предполагается возможность контроля цепей между барьером и системой ПАЗ, а также невозможно различить, какой из выходов барьера при размыкании переводит выходной шлейф в безопасное состояние. При необходимости можно реализовать контроль цепей подключения барьера к системе ПАЗ, например, одним из двух способов, приведенных ниже.

Версия 3

На Рисунок 3 показана схема с контролем целостности цепей подключения, но без возможности различения сигналов «Выход 1» и «Ошибка 1» барьера при переходе шлейфа в безопасное состояние.

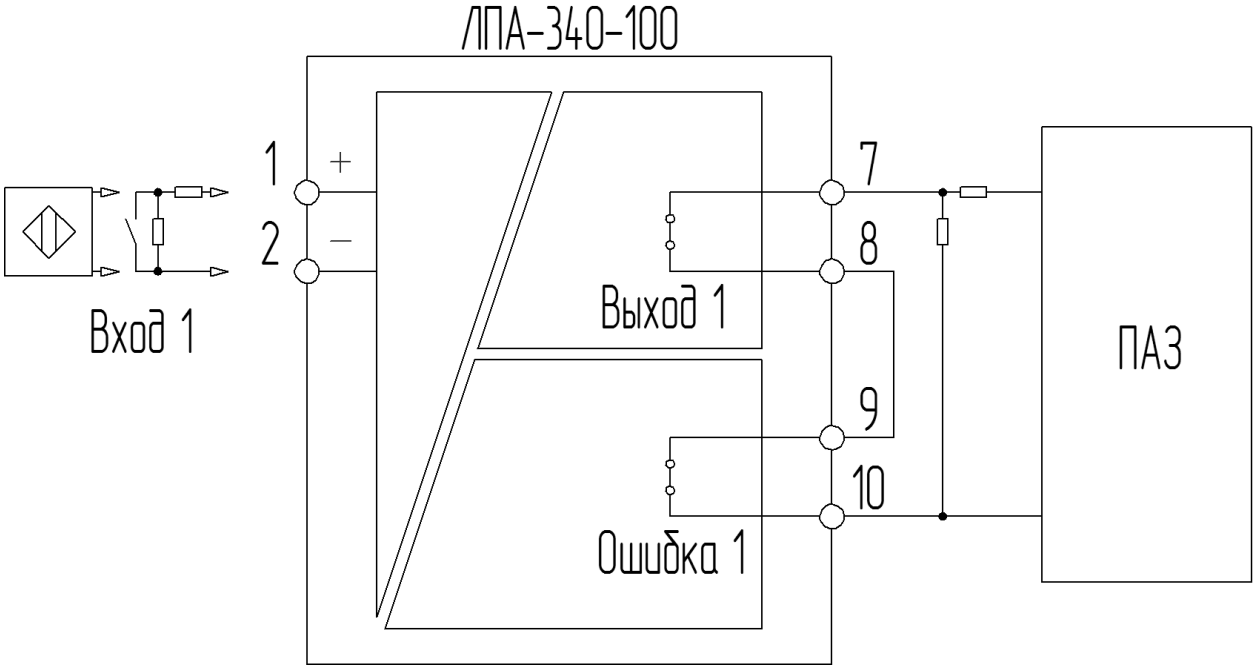

Рисунок 3 Подключение ЛПА-340-100 к системе ПАЗ единым шлейфом с контролем целостности, без различения ошибки барьера

На Рисунок 4 показана схема с контролем целостности цепей подключения и возможностью частичного различения сигналов «Выход 1» и «Ошибка 1» (в случае срабатывания сигнала «Ошибка 1» состояние сигнала «Выход 1» определить будет нельзя).

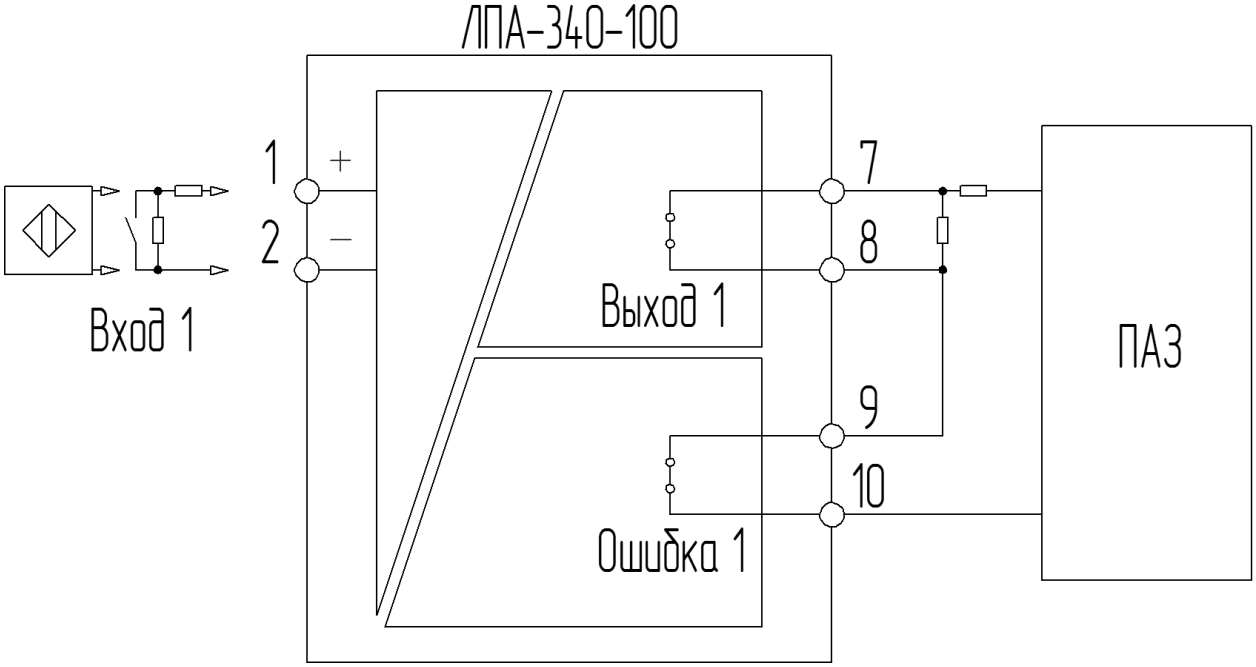

Рисунок 4 Подключение ЛПА-340-100 к системе ПАЗ единым шлейфом с контролем целостности, с различением ошибки барьера

Альтернативным вариантом реализации архитектуры 1001 является прием сигналов «Выход 1» и «Ошибка 1» независимо с их последующей логической обработкой на уровне системы ПАЗ. Здесь также можно в качестве примера привести два варианта (с контролем цепей подключения и без него).

На Рисунок 5 показана схема без контроля цепей подключения.

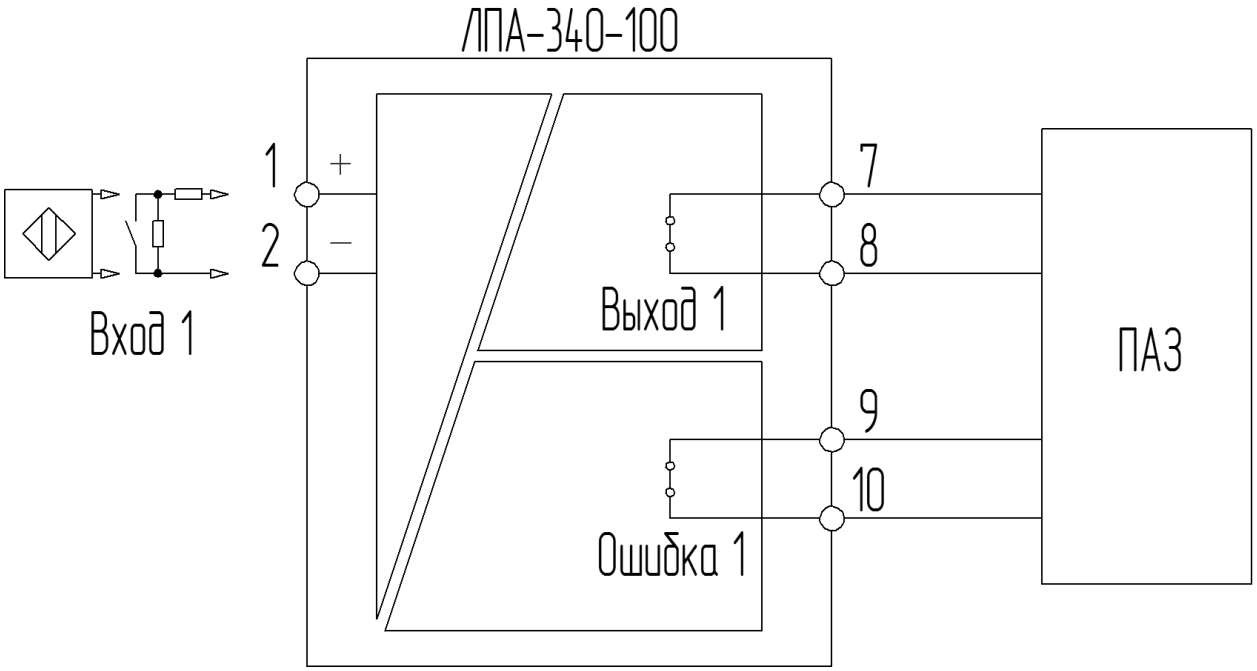

Рисунок 5 Подключение ЛПА-340-100 к системе ПАЗ независимыми шлейфами без контроля целостности, с различением ошибки барьера

На Рисунок 6 показана схема с контролем цепей подключения.

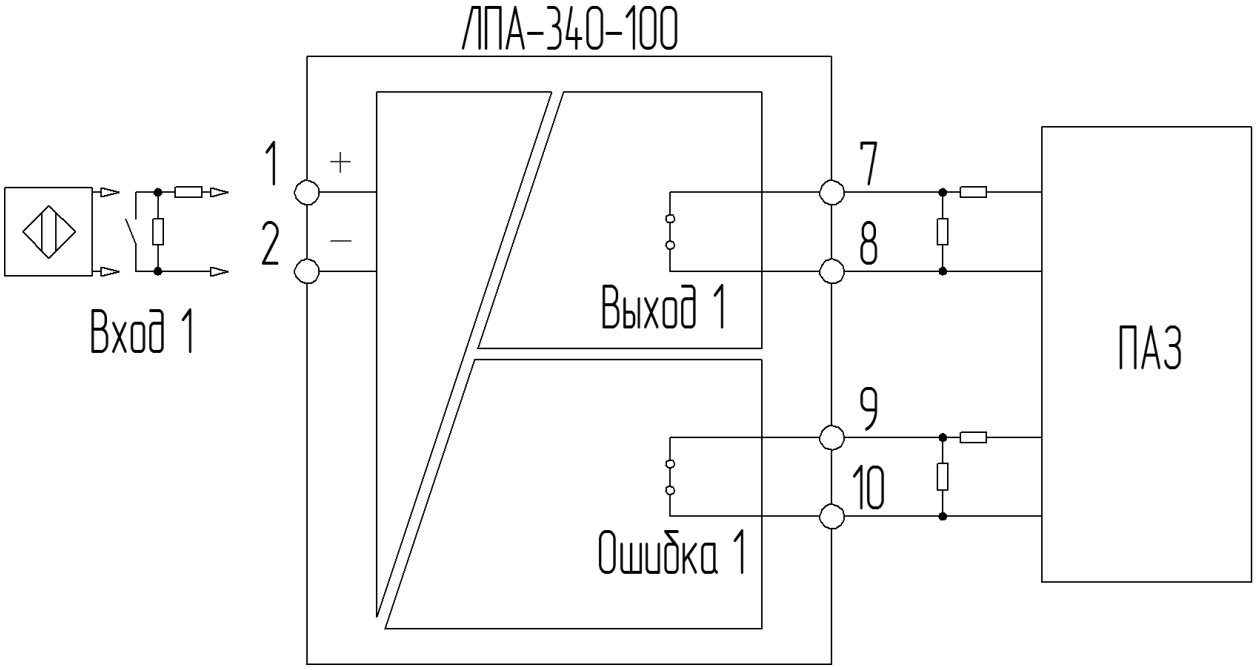

Рисунок 6 Подключение ЛПА-340-100 к системе ПАЗ независимыми шлейфами с контролем целостности, с различением ошибки барьера

Схемы, приведенные на Рисунок 3, Рисунок 4 и Рисунок 6, лишь иллюстрируют возможные варианты реализации контроля цепей. Поэтому в случаях, когда требуется

использовать контроль цепей подключения выходов барьера к системе ПАЗ или РСУ, оконечные элементы должны устанавливаться максимально близко к выходным клеммам барьера, а их тип, топология включения и характеристики должны выбираться строго в соответствие с требованиями документации на используемый контроллер.

Барьер ЛПА-340-220

В системе ПАЗ должен использоваться только первый канал барьера ЛПА-340-220. При использовании функции разветвления вход первого канала является ведущим, при этом второй выход (ведомый, дублирующий) может использоваться только в РСУ. Режимы инверсии выходов могут настраиваться независимо (см. Таблица 3). Если режим разветвления не используется, то второй канал может использоваться только в контуре РСУ, либо не использоваться вообще. На Рисунок 7 представлен вариант использования одного канала барьера в составе контура ПАЗ без разветвления, второй канал включен в контур РСУ.

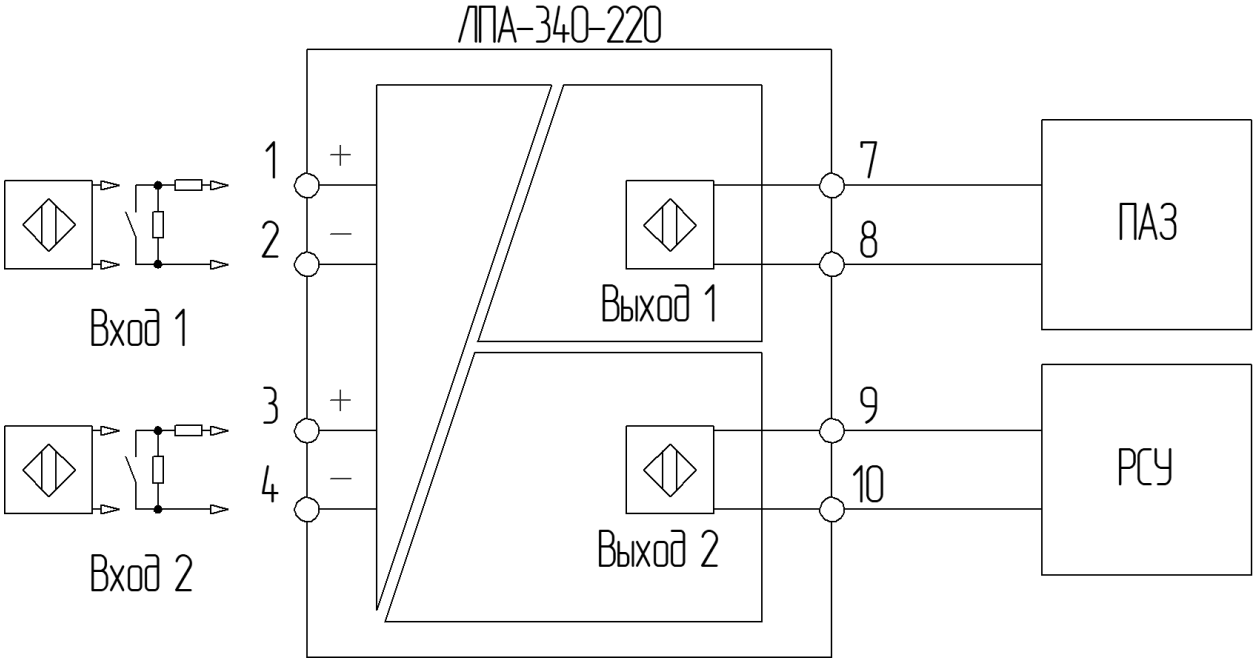

Рисунок 7 Подключение ЛПА-340-220 к системе ПАЗ (первый канал) без разветвления сигнала, второй канал используется в составе контура РСУ

На Рисунок 8 представлен вариант использования одного канала барьера в составе контура ПАЗ без разветвления, второй канал не используется.

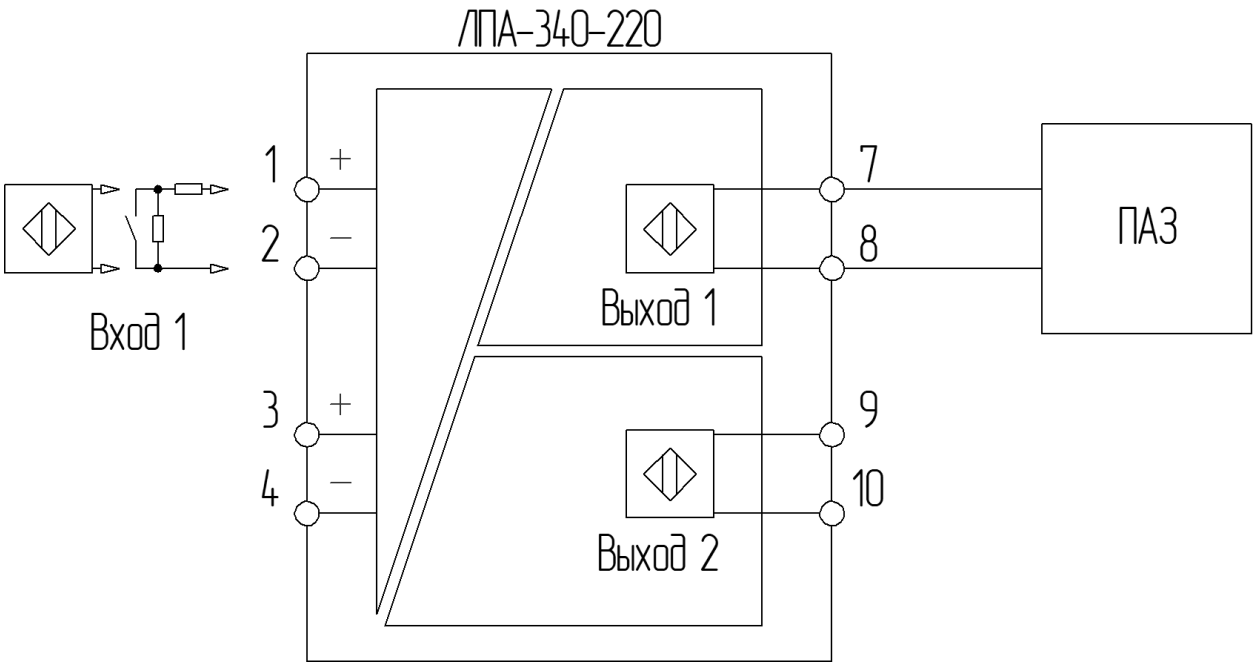

Рисунок 8 Подключение ЛПА-340-220 к системе ПАЗ)первый канал) без разветвления сигнала, второй канал не используется

На Рисунок 9 представлен вариант использования одного канала барьера в составе контура ПАЗ с разветвлением, второй выход (дублирующий) включен в контур РСУ.

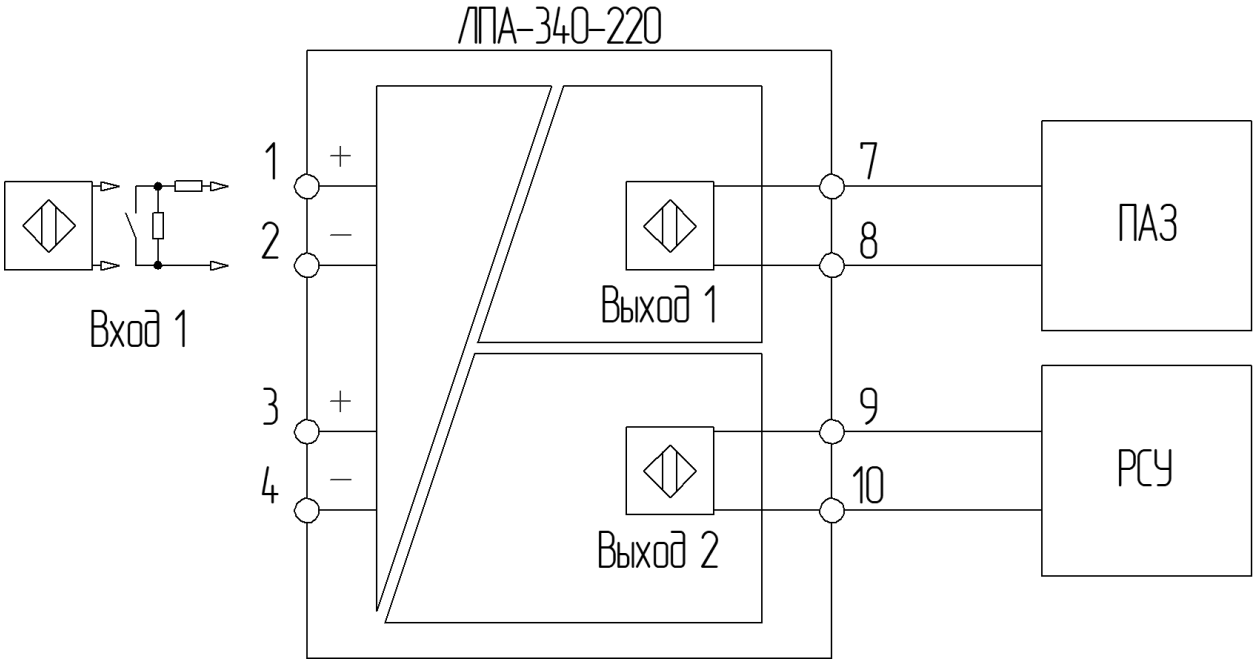

Рисунок 9 Подключение ЛПА-340-220 к системе ПАЗ с разветвлением сигнала, второй выход (дублирующий) используется в составе контура РСУ

Во всех случаях за счет формата выходных сигналов, соответствующих стандарту **NAMUR**, имеется возможность осуществлять контроль целостности цепей подключения выходов барьера независимо от того, куда они подключаются (в систему ПАЗ или РСУ).

6. Диагностика и обслуживание

6.1 Контрольные проверки

В соответствии с **ГОСТ Р МЭК 61508-2** 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).

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

Если результат проверки отрицательный, 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.

Проверка может проводиться в соответствие с одной из процедур, приведенных ниже.

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.

6.2 Состав контрольных проверок

В качестве имитатора входного сигнала допускается использовать датчик, соответствующий стандарту **NAMUR** или датчик типа сухой контакт с контролем цепей (см. 3.3.1), укомплектованными элементами, позволяющими имитировать неисправности цепей подключения датчика.

Для контроля выходных сигналов барьеров ЛПА-340-100 можно использовать мультиметр в режиме измерения сопротивления (в замкнутом состоянии сопротивление канала оптореле не должно превышать 25 Ом, в разомкнутом состоянии сопротивление канала оптореле не должно быть менее 1 МОм). Для контроля состояния выходов барьеров ЛПА-340-220 следует использовать переключающий усилитель, соответствующий стандарту **NAMUR**. Допускается также использовать входные цепи другого, заведомо исправного барьера (например, ЛПА-340-100).

Для питания проверяемого барьера и имитации неисправностей, связанных с источником внутреннего искробезопасного питания барьера, необходимо использовать регулируемый источник питания постоянного тока с возможностью установки выходного напряжения от 10 В до 25 В, нагрузочной способностью по току не менее 100 мА.

Проверку прохождения различных сигналов и состояний линии связи с датчиком через барьеры (а также и работу индикации) проводят в соответствие с Таблица 2 (для ЛПА-340-100, см. 3.3.3) и Таблица 3 (для ЛПА-340-100, см. 3.3.3) во всех допустимых к применению в системе ПАЗ режимах. Данная проверка проводится при номинальном напряжении питания 24 В.

Проверку работы цепей диагностики питания проводят в соответствие с Таблица 2 (для ЛПА-340-100, см. 3.3.3) и Таблица 3 (для ЛПА-340-100, см. 3.3.3) во всех допустимых к применению в системе ПАЗ режимах, путем плавного снижения напряжение питания барьера до уровня 12 В (ориентировочное значение) и фиксации поведения барьеров.

Рекомендуется также оценить общие параметры потребления барьеров в соответствие с данными, указанными в РЭ.

Ожидаемые результаты

Поведение барьеров с точки зрения выполнения функции безопасности (в т. ч. передача входного сигнала на выход, параметры потребления, работа цепей диагностики) должно строго соответствовать данным, приведенным в настоящем РФБ и РЭ.

6.3 Ремонт

При обнаружении ошибок вся 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 барьера, 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 барьера
	Контроль параметров барьера на объекте
	Контрольная проверка с демонтажом барьера

Результаты проверки

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.

β – эффективность теста по выявлению опасных отказов.

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.