УДК 51-74

ТИПОВЫЕ ПРИМЕРЫ РАСЧЕТА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ

Ирина Александровна Можаева, к.т.н. (ООО «НТЦ СЗМА»),
Александр Абрамович Нозик, к.т.н. (АО «СПИК СЗМА»),
Александр Владимирович Струков доцент, к.т.н. (АО «СПИК СЗМА»)

Введение

Основной задачей государственной политики в области промышленной безопасности до 2025 года и на дальнейшую перспективу является развитие методов анализа опасности и оценки риска аварий на опасных производственных объектах ОПО [1]. Существующие нормативные требования в области промышленной безопасности требуют, чтобы разработка систем противоаварийной защиты (СПАЗ) осуществлялась на основании анализа опасности и работоспособности контуров безопасности [2]. При этом показатели надежности СПАЗ должны устанавливаться и проверяться не менее чем для двух типов отказов – отказов типа «несрабатывание» и отказов типа «ложное срабатывание».

Для расчета показателей надежности СПАЗ с учетом отказов типа «несрабатывание» стандарты серии МЭК 61508 описывают методы оценки и устанавливают количественные требования к показателям функциональной безопасности PFDavg и PFH для соответствия необходимому, полученному на основе анализа риска, уровню полноты безопасности (УПБ, SIL). Разработанные методики оценки и нормирование показателей надежности СПАЗ с учетом отказов типа «ложное срабатывание» в настоящее время отсутствуют.

Общей проблемой для расчетов надежности СПАЗ как с учетом отказов типа «несрабатывание», так и отказов типа «ложное срабатывание», является отсутствие справочных данных на надежности компонентов, которые могут быть использованы как на ранних этапах проектирования, когда неизвестен конкретный типономинал компонентов, так и в учебных целях при реализации учебных программ, связанных с надежностью и функциональной безопасностью СПАЗ.

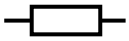
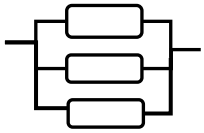
1. Упрощенная методика оценки вероятности и средней наработки до ложного срабатывания

Среди многочисленных публикаций на тему оценки вероятности ложных срабатываний СПАЗ [4, 7, 10] практически единогласно признается «дуальность» схем отказоустойчивости относительно отказов типа «несрабатывание» и отказов типа «ложное срабатывание». Например, физически ясно, что для снижения вероятности пропуска запроса на выполнение функции безопасности (ФБ) СПАЗ следует использовать резервирование, например, архитектуру 1oo2. В этом случае срабатывание ФБ произойдет, если запрос сформируется хотя бы в одном канале. С точки зрения ложного срабатывания архитектура 1oo2 является неэффективной, так как ложное срабатывание произойдет, если ложный сигнал появится в одном из каналов.

В то же время применение мажоритарной схемы 2oo3 практически не снижает вероятность отказа на запрос, но ложное срабатывание произойдет только при наличии ложного сигнала в двух каналах. Вероятность такого события крайне мала.

В табл.1 приведены примеры типовых архитектур подсистем СПАЗ в виде структурных схем надежности (ССН) и определены показатели отказоустойчивости по отношению к опасным и ложным отказам.

Таблица 1 – Показатели отказоустойчивости типовых схем [8]

Архитектура	ССН	Отказоустойчивость к опасным отказам (типа несрабатывание)	Отказоустойчивость к ложным отказам
1oo1		0	0
1oo2		1	0
2oo2		0	1
2oo3		1	1

В стандартах серии МЭК 61508 термин «ложное срабатывание» упоминается только один раз в разделе «Термины и определения» при описании безопасного отказа, который

а) приводит к ложному выполнению ФБ, переводящей управляемый объект (УО) или его часть в безопасное состояние или поддерживающей безопасное состояние, или

б) увеличивает вероятность ложного выполнения ФБ, переводящей управляемый объект или его часть в безопасное состояние или поддерживающей безопасное состояние.

Это определение не совсем согласуется с такими определениями, как опасная ситуация и опасное событие. Данные определения рассматривают возможность причинения вреда, в том числе и в виде физического повреждения или ущерба имуществу, что очень часто является следствием, например, ложной остановки процесса и затем ремонта оборудования. Тем более что, например, в перерабатывающей промышленности действия по пуску или остановке процесса являются источниками высокого риска.

В стандартах серии МЭК 61511 в разделе «Спецификация требований к безопасности ПСБ» указано, что требования должны включать максимально допустимую интенсивность ложных срабатываний. Тем не менее, стандарт не разъясняет, как определить эту интенсивность. В различных работах на тему функциональной безопасности приводятся не только разные формулы, но разные подходы к определению ложного срабатывания. Рассматриваются различные виды ложного срабатывания, зависящие, в первую очередь, от влияния этих отказов на процесс. С инженерной точки зрения влияние на технологический процесс обнаруженных опасных и безопасных отказов может быть совершенно различным. Необнаруженный безопасный отказ является скрытым отказом и в сочетании с другим отказом может привести к аварийной ситуации.

Следует согласиться, что определение частоты ложных срабатываний СПАЗ в значительной степени обуславливается принятым соглашением заинтересованных сторон [10]. Так, например, авторитетная независимая исследовательская организация SINTEF использует определение интенсивностей отказов типа «ложное срабатывание» λ_{SP} в виде выражения

$$\lambda_{SP} = \lambda_{SD} + \lambda_{SU} - \lambda_N, \quad (1)$$

где $\lambda_{SD}, \lambda_{SU}$ – обнаруженные и необнаруженные безопасные отказы;

λ_N – интенсивность отказов, не оказывающих непосредственного влияния на выполнение ФБ.

На наш взгляд, следуя требованию стандарта МЭК 61511 об определении максимально допустимой интенсивности ложных срабатываний, при оценке общей интенсивностей отказов типа «ложное срабатывание» следует учитывать интенсивность обнаруженных опасных отказов λ_{DD}. Тогда

$$\lambda_{SP} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD}. \quad (2)$$

В качестве показателя надежности СПАЗ относительно ложных срабатываний обычно используют либо среднюю наработку на ложный отказ $MTTF^{SP}$, либо частоту ложных тревог.

Так как одной из целей расчета надежности СПАЗ является сравнительный анализ схемно-конструктивного построения объекта и обоснование выбора рационального решения, предлагается методика оценки удобного для сравнения показателя ложных отказов – средней наработки на ложный отказ $MTTF^{SP}$.

Методика включает в себя два этапа:

1. Построение структурной схемы надежности СПАЗ с учетом отказоустойчивости относительно отказов типа «ложное срабатывание» (табл.1);
2. Ввод исходных данных о безотказности и ремонтопригодности элементов подсистем с учетом безопасных и обнаруженных опасных отказах.

Пример.

В качестве числового примера рассмотрим пример 1 из стандарта ГОСТ Р МЭК 61508-6 [3]. Архитектура системы рассматриваемого примера представлена на рис.1.

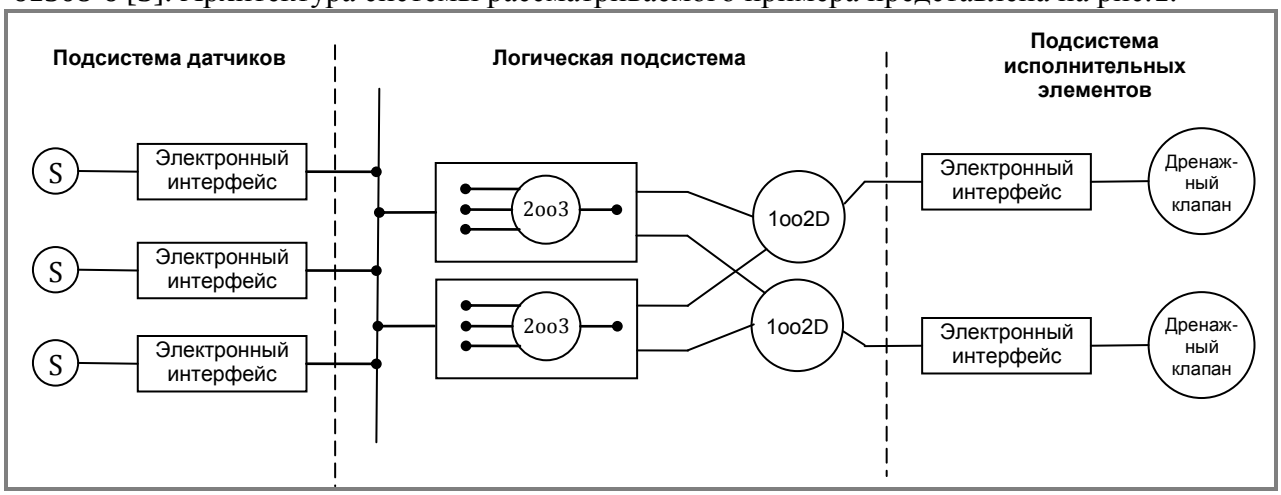


Рисунок 1 – Архитектура системы рассматриваемого примера из ГОСТ Р МЭК 61508-6

Исходные данные по компонентам системы безопасности приведены в табл.2.

Таблица 2 – Исходные данные по компонентам

Наименование элементов	λ_D (1/ч)	DC (%)	λ_{DU} (1/ч)	λ_S (1/ч)	$MTTF^{SP}$ (год)	T_1 (мес)	MTR (ч)
Датчики	2.5E-6	90	2.5E-7	2.5E-6	24.03	12	8
ПЭ логические элементы	5.0-6	99	5.0E-8	5.0-6	11.47	12	8
Дренажный клапан	2.5E-6	60	1.0E-6	2.5E-6	28.54	12	8
Закрывающий клапан	5.0E-6	60	2.0E-6	5.0E-6	14.27	12	8

В табл.2 приняты следующие обозначения:

λ_D – интенсивность опасных отказов, 1/ч;

DC – охват диагностикой, то есть часть опасных отказов, выявляемых автоматическими диагностическими тестами в неавтономном режиме, %;

λ_{DU} – интенсивность опасных необнаруженных отказов, $\lambda_{DU} = \lambda_D (1 - DC/100)$, 1/ч;

λ_S – интенсивность безопасных отказов, $\lambda_S=\lambda_D$ по предположения стандарта ГОСТ Р МЭК 61508-6, 1/ч;

$MTTF^{SP}$ – средняя наработка до отказа типа «ложное срабатывание»,

$$MTTF^{SP} = 1 \Big/ (\lambda_S + \lambda_D - \lambda_{DU}), \text{ год;}$$

T_1 – интервал времени между контрольными проверками, мес;

MTR – среднее время ремонта, ч.

На рис.2 показана структурная схема надежности СПАЗ с учетом характеристик отказоустойчивости структур, приведенных в табл.1.

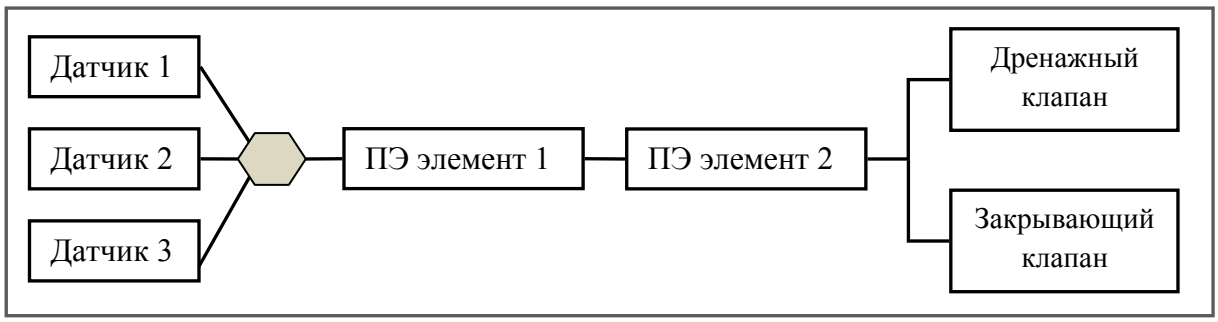


Рисунок 2 – Структурная схема надежности СПАЗ для расчета средней наработки на ложный отказ

На рис.2 архитектура 2oo3 датчиков для оценки надежности подсистемы с учетом отказов типа «ложное срабатывание» осталась неизменной по отношению к расчетной схеме (рис.1) для расчета PFDavg [5]. Это свойство называют зеркальностью поведения архитектур типа MooN [4, 8] по отношению к опасным отказам.

Архитектура 1oo2D логической подсистемы для задач оценки ложных срабатываний преобразуется в структуру 2oo2.

Архитектура подсистемы исполнительных механизмов из архитектуры 2oo2 для опасных отказов преобразуется в архитектуру 1oo2 для ложных отказов.

На рис.3 приведена расчетная схема функциональной целостности (СФЦ), реализованная в программной среде ПК АРБИТР [6].

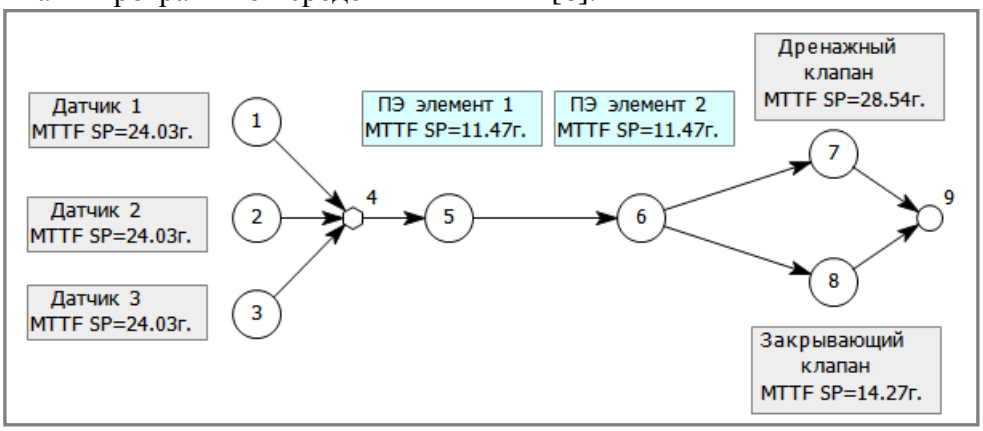


Рисунок 3 – СФЦ для расчета средней наработки на ложный отказ СПАЗ

Результаты расчетов надежности СПАЗ представлены на рис.4.

Расчет выполнен в вероятностно-временном режиме моделирования с заданной наработкой t=1год=8760час.

Результаты показали, что

- средняя наработка СПАЗ на ложный отказ $MTTF^{SP}$=5.735(г);
- средняя частота отказов – Wc=1.99E-05(1/ч);
- ожидаемое число отказов за 1 год – 0.174;
- общее суммарное время простоя системы – 1.395 час.

$КГ_{с}$ = **0.999840772531** - коэффициент готовности/неготовности системы
$T_{ос}$ = **50235** час (5.735 год) - средняя наработка на отказ
$T_{вс}$ = **8.000** час - среднее время ремонта (восстановления) системы
$P_{вс}(8760)$ = **0.839976059** - вероятность безотказной работы восстанавливаемой системы
$W_{с}$ = **0.174** 1/год (1.9903E-5 1/час) - частота отказов
TDT = **1.395** час - общее (суммарное) время простоя системы
$N_{ож.отк.}$ = **0.174** - ожидаемое число отказов

Рисунок 4 – Результаты расчета надежности СПАЗ

На рис.5 показаны результаты анализа характеристик значимости элементов СПАЗ.

Таблица характеристик элементов							
Номер эл-та	P эл-та	To эл-та	Тв эл-та	Значимость эл-та	Отрицательн. вклад	Положительн. вклад	Наименование
1	0.999961997	24.03	8	7.5991E-5	7.5988E-5	2.8879E-9	D1
2	0.999961997	24.03	8	7.5991E-5	7.5988E-5	2.8879E-9	D2
3	0.999961997	24.03	8	7.5991E-5	7.5988E-5	2.8879E-9	D3
5	0.999920386	11.47	8	0.99992	0.99984	7.9607E-5	ПЭ1
6	0.999920386	11.47	8	0.99992	0.99984	7.9607E-5	ПЭ2
7	0.999968002	28.54	8	6.3983E-5	6.3981E-5	2.0473E-9	Кл1
8	0.999936007	14.27	8	3.1993E-5	3.1991E-5	2.0473E-9	Кл2

Рисунок 5 – Характеристики значимости элементов СПАЗ

Из рис.5 видно, что наиболее значимыми элементами СПАЗ являются элементы контроллера (ПЭ1 и ПЭ2). Это объясняется их положением в структуре СПАЗ – при ложном срабатывании любого элемента контроллера может произойти ложное срабатывание ПАЗ.

Для срабатывания СПАЗ при ложных отказах датчиков и клапанов необходимо, чтобы отказали как минимум два датчика или два клапана. Вероятность одновременного отказа типа «ложное срабатывание» датчиков и клапанов значительно меньше аналогичных отказов элементов котроллера.

Для оценки влияния архитектуры датчиков на показатели надежности СПАЗ заменим архитектуру 2оо3 на дублирование. С точки зрения архитектуры, учитывающей влияние отказов типа «ложное срабатывание», дублированная система трансформируется в архитектуру 2оо2.

СФЦ для расчета надежности СПАЗ с измененной архитектурой подсистемы датчиков показана на рис.6.

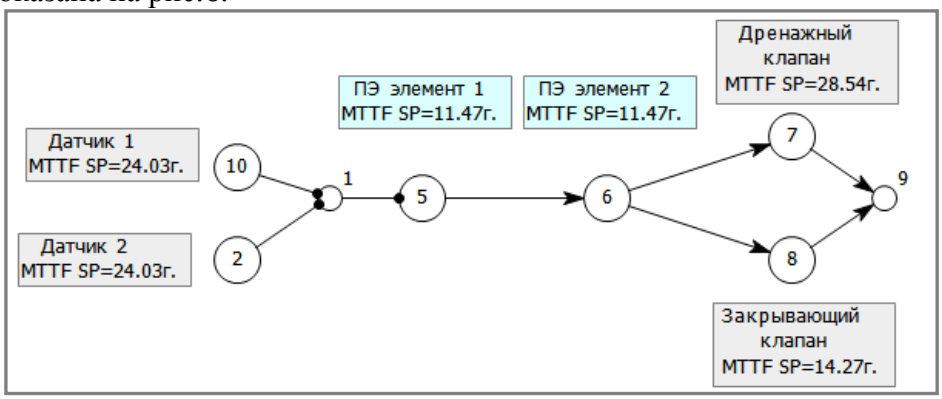


Рисунок 6 – СФЦ для расчета средней наработки на ложный отказ СПАЗ с измененной архитектурой

В табл.3 приведены сравнительные данные расчета надежности СПАЗ при разных архитектурах подсистемы датчиков.

Таблица 3 – Показатели надежности СПАЗ для разных подсистем датчиков

Показатель надежности СПАЗ	Архитектура подсистемы датчиков	
	2оо3	1оо2
средняя наработка СПАЗ на ложный отказ $MTTF^{SP}$(г)	5.735	3.882
средняя частота отказов – *Wc*, (1/ч)	1.99E-05	2.945E-05
ожидаемое число отказов за 1 год	0.174	0.258
общее суммарное время простоя системы, час	1.395	2.060

Изменение архитектуры подсистемы датчиков не только привело к ухудшению показателей надежности СПАЗ по ложным отказам, но и изменило соотношение значимостей элементов. В табл.4 представлены упорядоченные данные о значимостях элементов СПАЗ при различных архитектурах подсистемы датчиков.

Из табл.4 видно, что изменение архитектуры подсистемы датчиков изменило соотношение значимостей элементов СПАЗ. Если при структуре подсистемы датчиков 2оо3 наименее значимыми были датчики, то при изменении структуры наименее значимыми стали клапаны.

Таблица 4 – Показатели значимости элементов СПАЗ для разных подсистем датчиков

2oo3		1oo2	
Наименование элементов	Значимость	Наименование элементов	Значимость
ПЭ1	0.99992	ПЭ1	0.99984
ПЭ2	0.99992	ПЭ2	0.99984
Кл1	6.40E-05	D2	0.9998
Кл2	3.20E-05	D1	0.9998
D1	1.44E-09	Кл1	6.40E-05
D2	1.44E-09	Кл2	3.20E-05
D3	1.44E-09		

2. Примеры статистических данных о показателях надежности компонентов СПАЗ

Статистические данные о диапазоне значений средней наработки на опасный отказ $MTTF^D$ и отказ типа «ложное срабатывание» $MTTF^{SP}$ на предприятиях химической промышленности США в 2015 году для полевого оборудования и элементов логических устройств приведены в табл.5 [8].

Таблица 5 – Показатели надежности элементов СПАЗ для разных подсистем датчиков

Наименование оборудования	$MTTF^D$ (г)		$MTTF^{SP}$ (г)	
	min	max	min	max
Анализатор	0.35	4.00	0.35	4.00
Реле расхода (сигнализатор)	25	50	10	50
Датчик расхода	50	75	25	80
Реле уровня (сигнализатор)	25	125	15	75
Датчик уровня	25	250	15	150
Реле давления (сигнализатор)	15	80	15	80
Датчик давления	75	200	75	125
Реле температуры (сигнализатор)	10	100	10	50
Датчик температуры	75	250	25	100
Клапан соленоидный	30	100	10	30
Отсечной клапан	25	100	50	200
Управляющий клапан	50	60	30	100
Реле	100	1000	100	500
Пороговый усилитель (программ.)	300	600	150	275
Пороговый усилитель (непрограм.)	500	850	150	250
Программируемый контроллер по функционально безопасной технологии, один канал	100	250	5	15
Программируемый контроллер без функционально безопасной технологии, один канал	10	30	10	30

Исходные данные, приведенные в табл.1-5, используются для ориентировочных расчетов показателей функциональной безопасности на ранних этапах проектирования при отсутствии точных данных о номенклатуре элементов.

Использование минимальных и максимальных оценок интенсивности отказов, доли безопасных отказов и диагностического покрытия для безопасных и опасных отказов могут быть использованы для оценки неопределенности расчетов.

Таблицы 6 и 7 содержат исходные данные для типовых элементов систем с программируемой электроникой (ПЭ-систем).

Таблицы 8 и 9 содержат исходные данные для типовых элементов систем электрических и электронных (Э/Э-систем).

Таблица 6 – Исходные данные об интенсивности отказов и ДБО элементов ПЭ-систем [9]

Наименование элементов	Интенсивность отказов, $*10^6$ час			Доля безопасных отказов, %		
	min	avg	max	min	avg	max
Основной процессор	25.00	50.00	100.00	40	50	60
Процессор ввода/вывода	2.50	5.00	10.00	40	50	60
Модуль дискретного ввода	0.10	0.20	0.40	25	50	75
Модуль дискретного вывода	0.10	0.20	0.40	25	50	75
Источник (блок) питания	2.50	5.00	10.00	80	90	100
Сенсор (датчик)	2.00	13.00	42.00	20	40	60
Исполнительный элемент	2.00	13.00	42.00	20	40	60
Систематические отказы	0.10	1.00	10.00	20	50	60
Коэффициент модели отказов по общим причинам (ООП)		0.0225				

Таблица 7 – Исходные данные о диагностическом покрытии элементов ПЭ-систем [9]

Наименование элементов	Диагностическое покрытие, %					
	Безопасные отказы			Опасные отказы		
	min	avg	max	min	avg	max
Основной процессор	50	90	99	70	80	99
Процессор ввода/вывода	70	85	99	60	75	99
Модуль ввода/ вывода	0	50	99.9	0	25	99.9
Источник (блок) питания	90	95	99.9	0	0	99.9
Сенсор (датчик)	0	50	90	0	50	90
Исполнительный элемент	0	50	90	0	50	90

Таблица 8 – Исходные данные об интенсивности отказов и ДБО элементов Э/Э-систем [9]

Наименование элементов	Интенсивность отказов, $*10^6$ час			Доля безопасных отказов , %		
	min	avg	max	min	avg	max
Реле промышленные	0.20	0.50	2.00	50	75	90
Электромеханические таймеры	1.50	2.50	5.00	30	50	70
Твердотельный модуль ввода	0.10	0.20	0.40	25	50	75
Твердотельный модуль вывода	0.10	0.20	0.40	25	50	75
Твердотельный логический модуль	0.01	0.10	0.20	25	50	75
Твердотельный таймер	0.10	1.00	2.00	25	50	75
Твердотельный отказобезопасный модуль ввода	0.05	0.10	0.20	99.9	99.9	100
Твердотельный отказобезопасный модуль вывода	0.10	0.20	0.4	99.9	99.9	100
Твердотельный отказобезопасный логический модуль	0.001	0.01	0.1	99.9	99.9	100
Источник (блок) питания	2.50	5.00	10.00	100	100	100
Аналоговый пороговый усилитель	0.20	0.40	0.80	25	50	75
Сенсор (датчик)	2.00	13.00	42.00	20	40	60
Исполнительный элемент	2.00	13.00	42.00	20	40	60
Функциональные отказы	0.10	1.00	10.00	20	50	60

Таблица 9 – Исходные данные о диагностическом покрытии элементов Э/Э-систем [9]

Наименование элементов	Диагностическое покрытие, %					
	Безопасные отказы			Опасные отказы		
	min	avg	max	min	avg	max
Твердотельный модуль ввода	0	50	99.9	0	25	99.9
Твердотельный модуль вывода	0	50	99.9	0	25	99.9
Твердотельный логический модуль	0	50	99.9	0	25	99.9
Твердотельный таймер	90	95	99	0	0	99
Твердотельный отказобезопасный модуль ввода	25	50	90	-	-	-
Твердотельный отказобезопасный модуль вывода	25	50	90	-	-	-
Твердотельный отказобезопасный логический модуль	25	50	90	-	-	-
Аналоговый пороговый усилитель	0	50	99.9	0	25	99.9
Блок питания	90	95	99.9	0	0	99.9
Сенсор (датчик)	25	50	90	25	50	90
Исполнительный элемент	25	50	90	25	50	90

ЛИТЕРАТУРА

1. Указ президента РФ № 198 от 6 мая 2018 г. «Об Основах государственной политики Российской Федерации в области промышленной безопасности на период до 2025 года и дальнейшую перспективу».
2. Приказ Ростехнадзора от 11.03.2013 N 96 «Об утверждении Федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств».
3. ГОСТ Р МЭК 61508-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6.
4. Федоров Ю.Н. Основы построения АСУТП взрывоопасных производств. В 2-х томах. Т.1. «Методология» – М.:СИНТЕГ, 2006. 720 с.
5. Ветлугин К.А., Можаева И.А., Струков А.В. Программно-методическое обеспечение проектной оценки показателей функциональной безопасности систем противоаварийной защиты опасных производственных объектов // Сборник трудов двадцатой Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности» том 2, «Технические средства противодействия терроризму», РАРАН-Москва, НПО СМ - СПб., 2017, с.7083.
6. Можаев А.С. Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб.– М. : РНЦ «Курчатовский институт», 2008. – Вып. 2/2008. С.105-116.
7. Rausand M. Reliability of Safety-Critical Systems: Theory and Applications. Willey. 2014. 448 p.
8. Guedelines for Safe Automation of Chemical Process. CCPS, AIChE, 2017, New York, WILEY. P.633
9. ISA-dTR84.02. E/E/PE Systems for use in safety application – Safety Integrety Evalution Tecniques. ISA, 1995.
10. SINTEF Report «Reliability Prediction Method for Safety Instrumented Systems". PDS Example collection, 2010 Edition.