АЛГОРИТМЫ РАСЧЕТА ПОКАЗАТЕЛЕЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ

МОЖАЕВА И.А., НОЗИК А.А., СТРУКОВ А.В.
АО «СПИК СЗМА», С-Петербург, E-mail: info@szma.com

Аннотация

Рассматриваются примеры использования алгоритмов расчета показателей функциональной безопасности систем автоматической противоаварийной защиты (СПАЗ) с учетом отказов типа «несрабатывание» и типа «ложное срабатывание». Показаны возможности использования как метода анализа деревьев неисправностей, так и структурных схем надежности, позволяющих учитывать влияние отказов по общей причине. Программная реализация алгоритмов оценки показателей надежности СПАЗ выполнена в программной среде ПК АРБИТР. Приведены примеры расчетов показателей функциональной безопасности.

Ключевые слова: Система автоматической противоаварийной защиты, схема функциональной целостности (СФЦ), программный комплекс АРБИТР, структурно-сложные системы, отказы по общей причине (ООП), отказы типа «несрабатывание» и типа «ложное срабатывание», вероятность отказа на запрос, вероятность ложного срабатывания.

Введение

Существующие нормативные требования в области промышленной безопасности требуют, чтобы разработка систем противоаварийной защиты осуществлялась на основании анализа опасности и работоспособности контуров безопасности [1]. При этом показатели надежности СПАЗ должны устанавливаться и проверяться не менее чем для двух типов отказов – отказов типа «несрабатывание» и отказов типа «ложное срабатывание». Известны алгоритмы и методики оценки вероятности несрабатывания СПАЗ при низкой и высокой частоте запросов [2] и их программная реализация [7]. Общеприняты количественные требования к показателям функциональной безопасности для указанных режимов – средняя вероятность отказа на запрос PFDavg и средняя частота опасных отказов PFH, введены соответствующие уровни полноты безопасности (УПБ, SIL) [2].

Разработанные методики оценки и нормирование показателей надежности СПАЗ с учетом отказов типа «ложное срабатывание» в настоящее время отсутствуют.

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 по 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 Методологическая и алгоритмическая основы оценки вероятности отказа на запрос

По физическому смыслу *PFDavg* есть средняя неготовность системы на интервале между контрольными проверками. Расчет *PFDavg* основан на учете двух типов неготовности канала:

1 – неизвестная, когда простой СПАЗ вызван DD (опасными необнаруженными) или DU (опасными обнаруженными) отказами;

2 – неизвестная, когда простой вызван тестовыми проверками, плановыми ремонтами и т.п., когда можно включить другие слои защиты.

Алгоритмическая основа методики оценки *PFDavg* различных архитектур – приближенные формулы стандарта IEC 61508-6 для расчета *PFDavg* простых типовых архитектур 1oo1 и 1oo2D [2].

Основная идея IEC 61508-6 состоит в расчете *PFDavg* канала, представленного как один элемент, характеризуемый средней групповой частотой опасных отказов λ_{DG} и эквивалентным групповым временем простоя t_{GE} [9]

$$PFD_{avg}^{(G)} = F(\lambda_{DG}, t_{GE}, MTTR, MRT).$$

Так как состояние системы безопасности полностью определяется состоянием ее элементов, то системный показатель ФБ рассчитывается с использованием структурной функции системы, то есть

$$PFD_{sys} = P\{PFD_1, \dots, PFD_i, \dots, PFD_n\},$$
$$PFH_{sys} = P\{PFH_1, \dots, PFH_i, \dots, PFH_n\},$$

где *PFDsys*, *PFHsys* – системные показатели;

PFDi, *PFHi* – показатели ФБ *i-го* компонента;

P{…} – структурная функция системы.

В общем виде методика расчета *PFDavg* канала включает в себя следующие шаги [7,8]:

I. Формирование исходных данных, необходимых для расчета вероятностей отказа на запрос для всех элементов системы.

II. Расчет с помощью специализированной утилиты ввода исходных данных вероятностей отказа на запрос структур с архитектурой 1oo1 и 1oo2D по формулам стандарта ГОСТ Р МЭК 51508-6.

III. Построение схемы функциональной целостности в виде структурной схемы надежности (ССН) или дерева неисправностей (ДН) и моделирование надежности СПАЗ с учетом особенностей построения голосующих групп в программной среде ПК АРБИТР [4,5].

Формирование исходных данных, необходимых для расчета показателей функциональной безопасности, осуществляется на основе анализа документации производителей компонентов каналов СПАЗ.

Для иллюстрации методики расчета *PFDavg* канала рассмотрим пример 1 [2]. На рис.1 представлена структурная схема СПАЗ.

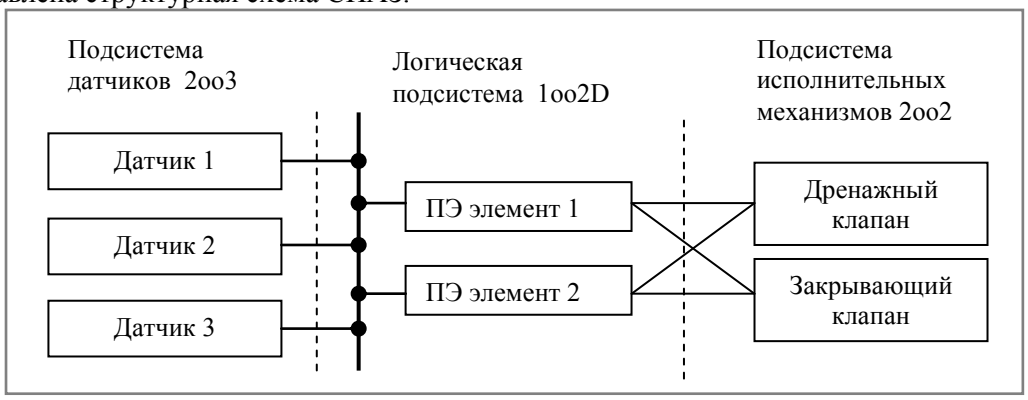


Рисунок 1 – Структурная схема СПАЗ [2]

Анализируемая система безопасности включает в себя голосующую группу аналоговых датчиков давления (датчики 1-3) с архитектурой 2oo3 на выходе. Логическая подсистема включает в себя два программируемых электронных элемента с архитектурой 1oo2D, управляющие сигналы которых поступают на дренажный и закрывающий клапаны. Для обеспечения функции безопасности необходима работа обоих клапанов.

На рис.2 представлена схема функциональной целостности для моделирования надежности голосующей группы датчиков с архитектурой 2oo3 с учетом отказов по общей причине с использованием модели бета-фактора.

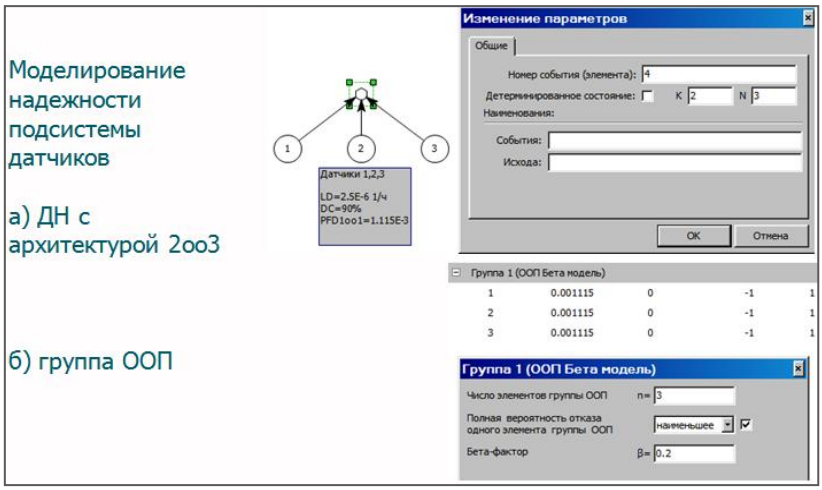


Рисунок 2 – СФЦ подсистемы датчиков [7]

На рис.3 показана окончательная СФЦ системы безопасности и результаты моделирования по исходным данным, заданным в стандарте МЭК 61508-6.

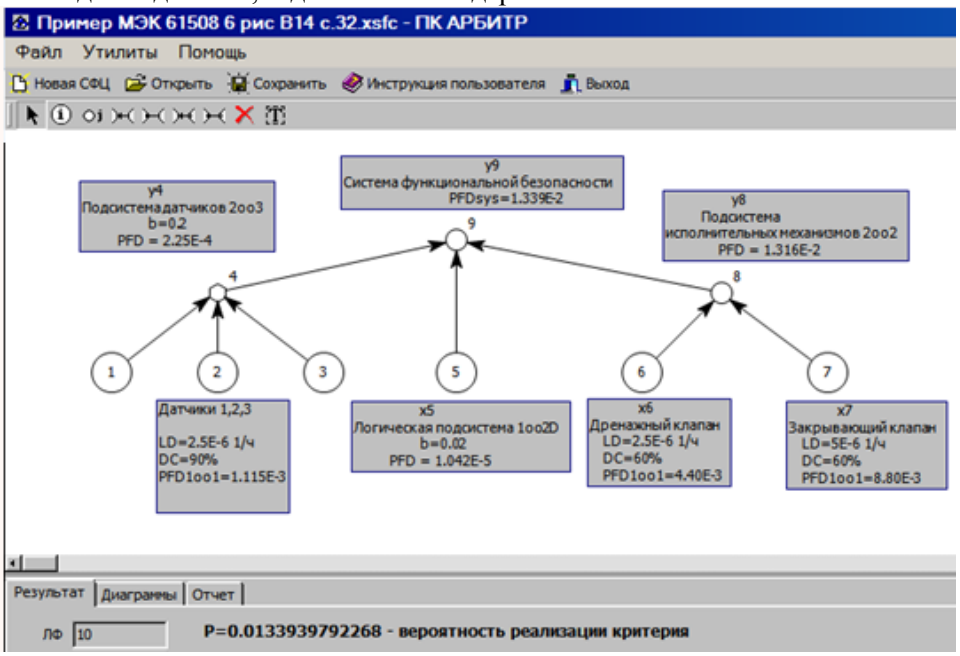


Рисунок 3 – СФЦ системы безопасности [7]

Как видно из рис.11, *PFDsys* системы безопасности составляет 1.33E-2, что соответствует уровню полноты безопасности SIL1 и совпадает с решением, приведенным в [2].

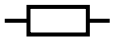
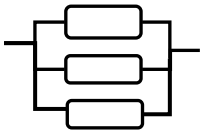
2 Упрощенная методика оценки вероятности и средней наработки до ложного срабатывания

Среди публикаций на тему оценки вероятности ложных срабатываний СПАЗ практически единогласно признается «дуальность» схем отказоустойчивости относительно отказов типа «несрабатывание» и отказов типа «ложное срабатывание» [6,9,10,12]. Например, 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 и определены показатели отказоустойчивости по отношению к опасным и ложным отказам.

Таблица 1 – Показатели отказоустойчивости типовых схем [10]

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 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 [12] 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 (рис.1).

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»,

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

T_1 – интервал времени между контрольными проверками, мес;

MTR – среднее время ремонта, ч.

На рис.4 показана структурная схема надежности СПАЗ с учетом характеристик отказоустойчивости структур, приведенных в табл.1.

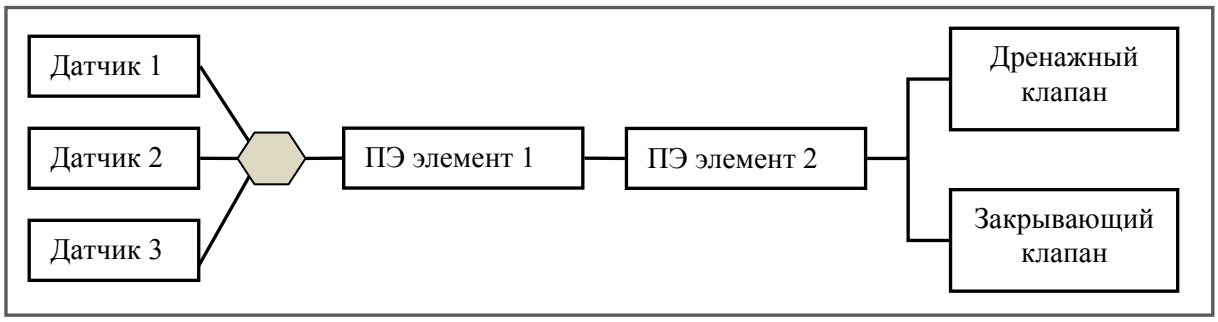


Рисунок 4 – Структурная схема надежности СПАЗ для расчета средней наработки на ложный отказ

На рис.4 архитектура 2oo3 датчиков для оценки надежности подсистемы с учетом отказов типа «ложное срабатывание» осталась неизменной по отношению к расчетной схеме (рис.2) для расчета PFDavg. Это свойство называют зеркальностью поведения архитектур типа MooN 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.5 приведена расчетная схема функциональной целостности (СФЦ), реализованная в программной среде ПК АРБИТР.

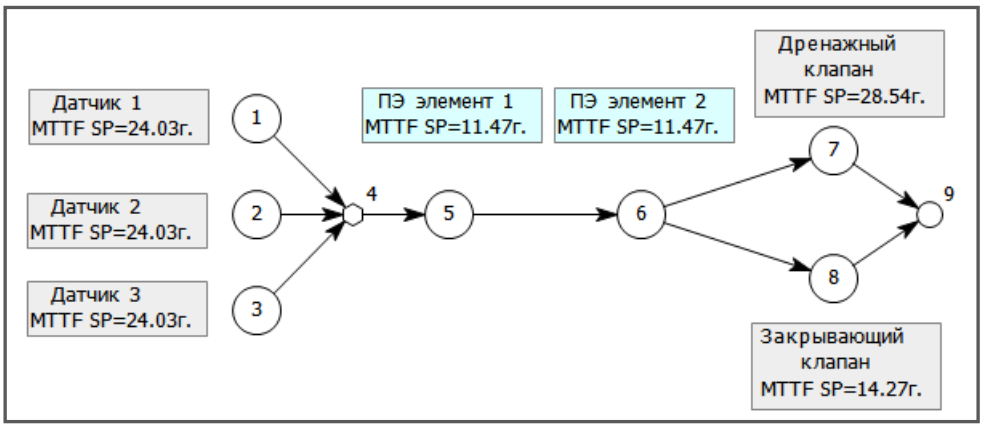


Рисунок 5 – СФЦ для расчета средней наработки на ложный отказ СПАЗ

Результаты расчетов надежности СПАЗ представлены на рис.6.

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.

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.

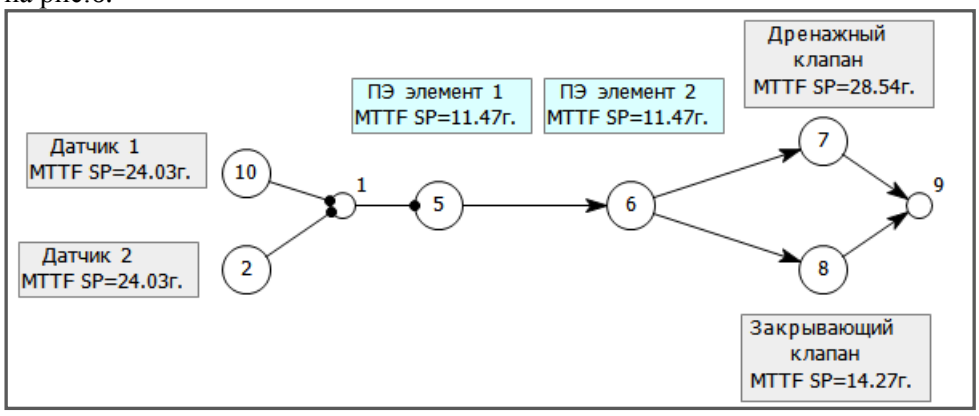


Рисунок 6– СФЦ для расчета средней наработки на ложный отказ СПАЗ с измененной архитектурой

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 естественно привело к ухудшению показателей надежности СПАЗ по ложным отказам.

Вывод

Особенностью алгоритма оценки вероятности отказа на запрос является формирование дерева неисправностей с учетом групп отказов по общей причине. При этом исходные данные для каждого элемента расчетной схемы формируются с помощью специализированной утилиты. Алгоритм расчета средней наработки на ложное срабатывание также включает в себя формирование расчетной схемы теперь уже в виде структурной схемы надежности, учитывающей отказоустойчивость по отношению именно к ложным срабатываниям. Подготовка исходных данных для каждого элемента схемы осуществляется с помощью элементарных преобразований.

Программная реализация алгоритмов расчета показателей функциональной безопасности СПАЗ осуществлена в программной среде ПК АРБИТР.

Практическое применение описанных алгоритмов должно также учитывать особенности влияния ложных срабатываний СПАЗ на конкретный технологический процесс.

Литература

1 ФНиП «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств», утверждены приказом Ростехнадзора №96 от 11.03.2013 г.

2 ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1-7. 2012.

3 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.

4 Программный комплекс АРБИТР. URL: www.szma.com/pkasm.shtml.

5 Федоров Ю.Н. Основы построения АСУТП взрывоопасных производств. В 2-х томах. Т.1. «Методология» – М.:СИНТЕГ, 2006, 720 с.

6 Можаева И.А., Струков А.В. Применение ПК АРБИТР для проектной оценки показателей функциональной безопасности систем противоаварийной защиты// Труды 4-й Международной научно-практической конференции "Имитационное и комплексное моделирование морской техники и морских транспортных систем" (ИКМ МТМТС – 2017), С-Петербург, 2017, С.100–105.

7 К.А.Ветлугин, Можаева И.А, А.В.Струков. 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.70–83.

8 Rausand M. Reliability of Safety-Critical Systems: Theory and Applications. Willey. 2014. 448 p.

9 Guedelines for Safe Automation of Chemical Process. CCPS, AIChE, 2017, New York, WILEY. P.633.

10 ISA-dTR84.02. E/E/PE Systems for use in safety application – Safety Integrety Evalution Tecniques. ISA, 1995.

11 SINTEF Report «Reliability Prediction Method for Safety Instrumented Systems”. PDS Example collection, 2010 Edition.