МЕТОДЫ РЕШЕНИЯ ПРЯМОЙ И ОБРАТНОЙ ЗАДАЧИ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ПАЗ. ЧАСТЬ 1

И.А. Можаева, **А.А. Нозик, А.В. Струков** (АО «СПИК СЗМА»)

Введение

Методы, используемые для решения задач оценки функциональной безопасности (ФБ), могут быть объединены в две группы: статические (логические) и динамические (состояния/переходы) модели, а также аналитические модели и моделирование на основе метода Монте-Карло. В инженерной практике широкое применение получили логические методы, описывающие статические, независимые от времени, логические связи между отказами компонентов системы и полным отказом системы.

Упрощенный логический метод, который рассматривается в статье, основан на графическом представление структурной схемы надежности (ССН) или дерева неисправностей (ДН) с использованием дополнительных вычислений в виде специальной формулы Маркова, выведенной из работ Тейлора с учетом консервативных допущений, описанных в стандарте МЭК 61508-6–2012 [1]. Основной причиной использования моделей Маркова является возможность учета динамики изменения состояний системы во времени, например, учет периодических контрольных проверок.

В соответствии с рекомендациями [1] условием для применения логических моделей является отделение графического представления системы от вычислений. В этом случае ССН или ДН используются для моделирования надежности системы или условий отказа, а расчетные формулы – для оценки средней вероятности отказа на запрос (PFDavg). Важно отметить, что ССН и ДН представляют структуру системы дуальными (двойственными) логическими функциями и позволяют вычислять мгновенные значения надежности или неготовности системы. После этого может быть вычислено среднее значение показателей надежности за определенный интервал времени. Кроме того, общая методология оценки показателей функциональной безопасности систем противоаварийной автоматической защиты (ПАЗ) предполагает расчет средних значений показателей надежности/неготовности на межпроверочном интервале. Таким образом, динамическая задача сводится к решению статической, независимой от времени задачи вычисления мгновенной надежности/неготовности системы ПАЗ.

ССН могут эффективно использоваться для моделирования отказов типа «ложное срабатывание», а ДН – для моделирования отказов типа «несрабатывание» [4]. И в том и другом случае важным является правильное определение логических условий указанных событий, точное обозначение границ функционирования отдельных голосующих групп, где они объединяются с помощью процедуры голосования.

При использовании программных средств для оценки ФБ систем ПАЗ необходимо верифицировать программный продукт путем сравнения результатов нескольких тестовых примеров с результатами, полученными ручным способом, например, в среде Excel, с применением формул стандарта [1].

1 Верификация программного средства ПК АРБИТР для решения задач оценки функциональной безопасности

Верификация программного средства ПК АРБИТР [2] проводилась путем сравнения результатов расчета средней вероятности отказа на запрос *PFD*avg для режима с низкой интенсивностью запросов, полученных:

- в программной среде Excel с использованием формул раздела B.2 стандарта МЭК 61508-6–2012;
- при моделировании заданных структур в программной среде Reliability Workbench (RWB) [3].

Результаты оценки *PFD*avg, полученные в программной среде Excel, также дополнительно сравнивались с результатами, показанными в таблицах В.2–В.5 стандарта [1]. Необходимость такого сравнения вызвана наличием редакционных ошибок в изданном стандарте. Кроме того, расчеты в программной среде Excel позволяют получить большее число значащих цифр после запятой, что позволяет корректно осуществлять округление результатов.

По физическому смыслу вероятность отказа на запрос системы ПАЗ *PFD*avg есть средняя неготовность системы на интервале между контрольными проверками. Так как состояние системы ПАЗ полностью определяется состоянием ее элементов (каналов, подсистем), то элементами структурной функции, описывающей взаимосвязь системных показателей с показателями надежности элементов, будут показатели средней неготовности элементов, каналов и подсистем [4]. Таким образом, можно записать

$$PFDsys = P\{PFD_1,...,PFD_i,...,PFD_n\},$$

где $PFDsys$ – вероятность отказа на запрос системы ПАЗ;

PFD_i – вероятность отказа на запрос *i*-го компонента;

$P\{\cdots\}$ – структурная функция системы безопасности.

Таким образом, методика оценки вероятностей отказа на запрос и средней частоты опасных отказов аппаратных средств систем безопасности с применением ПК АРБИТР по содержанию совпадает с методикой количественных оценок надежности, которые выполняются на основе расчетных многочленов вероятностной функции, и состоит из пяти последовательно выполняемых этапов.

Этап I – выбор подхода к логико-вероятностной постановке задачи (прямого, обратного или комбинированного), формирование математической модели исследуемого свойства системы.

Этап II – первичное структурно-логическое моделирование.

Этап предполагает подготовку следующих исходных данных:

- структурной модели исследуемого свойства системы в форме СФЦ, в которой функциональными вершинами являются компоненты с архитектурой 1oo1 и 1oo2D, а эквивалентированными вершинами – все остальные компоненты;
- определение вероятностных параметров компонентов с помощью дополнительных вычислительных средств [5];
- задание логических критериев, определяющих на СФЦ условия реализации исследуемых свойств.

При необходимости формируются группы элементов с отказами по общей причине (ООП).

Этап III – построение логической функции.

Логическая функция определяется автоматически на основе СФЦ и заданного логического критерия. Важным на данном этапе является проверка соответствия полученных минимальных сечений реальным условиям отказа исследуемой системы ПАЗ.

Этап IV – построение вероятностной функции.

Построение вероятностной функции в форме правильных многочленов осуществляется автоматически.

Этап V – Выполнение расчетов системных характеристик, формирование отчета.

Данный этап анализа системы является завершающим.

Расчетные формулы для оценки вероятности отказа на запрос *PFD*avg для различных структур каналов ПАЗ [1] для режима с низкой интенсивность запросов приведены в табл.1

Таблица 1 – Формулы для расчета показателей безопасности *PFD*avg

Архитектура	Расчетная формула
1oo1	$PFD_{1oo1} = \lambda_{du}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{dd} \cdot MRT$ (1)
1oo2	$PFD_{1oo2} = 2\left(\left(1-\beta_D\right)\lambda_{DD} + \left(1-\beta\right)\lambda_{DU}\right)^2 t_{CE} t_{GE} + + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right),$ где $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR,$ $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR.$ (2)
1oo2D	$PFD_{1oo2D} = 2\left(1-\beta\right)\lambda_{DU}\left(\left(1-\beta\right)\lambda_D + \left(1-\beta_D\right)\lambda_{DD} + \lambda_{SD}\right)t_{CE'} t_{GE'} + + 2\left(1-K\right)\lambda_{DD} t_{CE} + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right),$ где $t_{CE'} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + \left(\lambda_{DD} + \lambda_{SD}\right)MTTR}{\lambda_{DU} + \left(\lambda_{DD} + \lambda_{SD}\right)},$ $t_{GE'} = \frac{T_1}{3} + MRT.$ (3)
2oo3	$PFD_{2oo3} = 6\left(\left(1-\beta_D\right)\lambda_{DD} + \left(1-\beta\right)\lambda_{DU}\right)^2 t_{CE} t_{GE} + + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right).$ (4)

В табл.1 использованы следующие обозначения (согласно табл. B1[1]):

T_1 – интервал времени между контрольными проверками, ч.;

MTTR – среднее время восстановления, ч.;

MRT – среднее время ремонта, ч.;

β – доля необнаруженных отказов по общей причине, %;

β_D – доля обнаруженных отказов диагностическими тестами и имеющих общую причину, $\beta=2\beta_D$, %;

λ_{DU} – интенсивность опасных необнаруженных отказов, отказ/ч.;

λ_{DD} – интенсивность опасных обнаруженных отказов, отказ/ч.;

λ_{SD} – интенсивность безопасных обнаруженных отказов, отказ/ч.;

t_{CE} – эквивалентное среднее время простоя канала для архитектур 1oo1, 1oo2, 2oo3,ч;

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

$t_{CE'}$ – эквивалентное среднее время простоя канала для архитектуры 1oo2D, ч;

$t_{GE'}$ – эквивалентное среднее время простоя голосующей группы для архитектуры 1oo2D, ч.

Основная идея формул стандарта [1], по мнению профессора Норвежского университета науки и технологий Marvin Rausand, состоит в том, что голосующая группа элементов (структура) представляется одним эквивалентным элементом с некоторой средней групповой (G) интенсивностью опасных (D) отказов $\lambda_{D,G}$ со средним временем простоя t_{GE} [6].

Пример с результатами сравнения представлен в табл.2.

Таблица 2 – Фрагмент сравнения результатов моделирования

Параметры моделирования: T_1=6 мес, MRT=MTTR=8ч, λ_d=0.5E-07 (1/ч), β=2%.

DC, %	Архитектура 1oo1	
	ГОСТ	**Excel/ RWB**
0	1.1E-04	1.099E-04
60	4.4E-05	4.42E-05
90	1.1E-05	1.135E-05
99	1.5E-06	1.495E-06

DC, %	Архитектура 1oo2				Архитектура 1oo2D			
	ГОСТ	**Excel**	**ПК**	**RWB**	**ГОСТ**	**Excel**	**ПК**	**RWB**
0	2.2E-06	2.213E-06	2.19E-06	2.21E-06	2.2E-06	2.213E-06	-	-
60	8.8E-07	8.841E-07	8.858E-07	8.859E-07	**1.4E-06**	**1.548E-06**	-	-
90	2.2E-07	2.236E-07	2.27E-07	2.271E-07	4.3E-07	4.418E-07	-	-
99	2.6E-08	2.594E-08	2.99E-08	2.99E-08	6.0E-08	5.961E-08	-	-

DC, %	Архитектура 2oo3				Архитектура 1oo3			
	ГОСТ	**Excel**	**ПК**	**RWB**	**ГОСТ**	**Excel**	**ПК**	**RWB**
0	2.2E-06	2.244E-06	2.233E-06	2.233E-06	2.2E-06	2.198E-06	2.198E-06	2.198E-06
60	8.9E-07	8.892E-07	8.896E-07	8.896E-07	8.8E-07	8.816E-07	8.84E-07	8.84E-07
90	2.2E-07	2.239E-07	2.274E-07	2.274E-07	2.2E-07	2.234E-07	2.27E-07	2.27E-07
99	2.6E-08	2.595e-08	2.99E-08	2.991E-08	2.6E-08	2.594E-08	2.99E-08	2.99E-08

В верхней части табл.2 приведены результаты расчетов показателя *PFD*avg для архитектуры 1oo1 (одиночный компонент). В столбце «ГОСТ» приведены результаты расчетов из табл. В2 стандарта [1], в столбце «Excel/ RWB» – результаты расчетов в среде Excel по формуле (1) табл.1 и в программе RWB. В программе RWB реализована возможность ввода исходных данных (T_1, MRT, MTTR, λd, *DC*) для расчета параметров ФБ отдельных элементов схем (ССН и ДН). Такая же возможность реализована и в ПК АРБИТР. Анализ данных в верхней части табл.2 показывает полное совпадение результатов расчетов.

В средней и нижней частях табл.2 приведены результаты расчетов для различных архитектур голосующих групп, часто используемых в системах ПАЗ. В столбцах «DC» приведены значения охвата диагностикой компонентов групп. В столбце «ГОСТ» приведены результаты расчетов из табл. В2 стандарта [1], в столбце «Excel» – результаты расчетов в среде Excel по формулам (2)-(4) табл.1, в столбцах «ПК» и «RWB» – результаты моделирования в программах ПК АРБИТР и RWB соответственно.

Моделирование в программах ПК АРБИТР и RWB осуществлялось в соответствии с рекомендациями стандарта [1]. Для каждого элемента группы рассчитывались параметры *PFD*avg по формуле (1) табл.1, как для структуры 1oo1. Затем графическими инструментами моделировалась необходимая архитектура (1oo2, 2oo3, 1oo3), вводились параметры учета отказов по общей причине (β-модель) и производился расчет параметра *PFD*avg для группы [5].

Параметры архитектуры 1oo2D рассчитывались только аналитически (по формуле (3) табл.1). Структурное моделирование архитектуры 1oo2D в программах ПК АРБИТР и RWB не представляется возможным.

Анализ данных, представленных в средней и нижней частях табл.2, позволяет сделать следующие выводы:

1 Результаты структурного моделирования в программах ПК АРБИТР и RWB совпадают.

2 Результаты структурного моделирования в программах ПК АРБИТР и RWB являются консервативными относительно результатов, приведенных в стандарте [1].

3 Расчеты в программной среде Excel обнаружили редакционную опечатку в данных для структуры 1oo2D (выделено жирным шрифтом).

Специалисты могут ознакомиться с полными таблицами сравнительных результатов расчетов в программной среде Excel и моделирования в программах ПК АРБИТР и RWB по запросу на адрес info@SZMA.com.

На основе полученных результатов и с учетом результатов практического применения утилиты [5] разработан дополнительный расчетный модуль, который может применяться как дополнительное вычислительное средство в составе ПК АРБИТР, или использоваться как самостоятельное вычислительное средство.

Расчетный модуль реализует три процедуры:

- расчет параметров *PFD*avg для архитектур 1oo1 и 1oo2D;
- оценку параметра β для модели отказов по общим причинам по методике, описанной в Приложении D стандарта [1];
- расчет параметров *PFD*avg канала системы ПАЗ по упрощенной методике.

2 Модуль для расчета параметров *PFD*avg для архитектур 1oo1 и 1oo2D

В зависимости от полноты и вида исходных данных о безотказности элементов расчеты могут проводиться на четырех страницах модуля.

Каждая страница содержит 3 раздела (фрейма) исходных данных (рис.1).

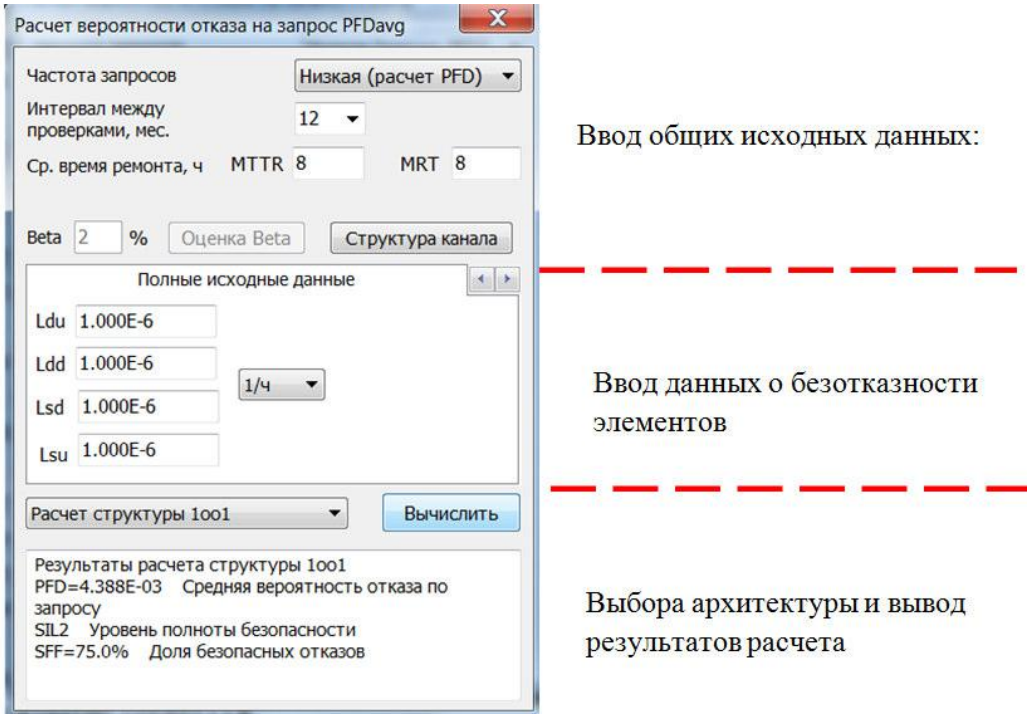


Рисунок 1 – Страница «Полные исходные данные» расчетного модуля

Верхний раздел (фрейм) является общим для всех страниц модуля. В нем задаются следующие параметры и режимы моделировании:

- Частота запросов: при низкой частоте запросов рассчитывается параметр средней вероятности отказа на запрос *PFD*avg, при высокой – средняя частота опасных отказов *PFH*.
- Интервал между проверками (T_1), задается в месяцах. Может быть выбрано одно из дискретных значений (1, 3, 6, 12, 24, 60) или вводиться любое другое положительное целое число.
- Среднее время ремонта в виде параметров *MTTR* или *MRT*, в ч.

Нижняя часть этого фрейма активируется при вводе параметров структуры 1oo2D или для перехода на страницу «Структура канала».

В зависимости от полноты и вида исходных данных о безотказности элементов возможны 4 варианта ввода исходных данных:

Вариант 1. «Полные исходные данные» предполагает ввод интенсивностей отказов (рис.1):

- Необнаруженных (undetected) опасных (dangerous) отказов *Ldu*;
- обнаруженных (detected) опасных отказов *Ldd*;
- безопасных (safety) обнаруженных отказов *Lsd*;
- безопасных необнаруженных отказов *Lsu*.

На все страницах модуля интенсивности отказов имеют размерности: 1/ч, 1/год, FIT (10^{-9}1/ч).

Вариант 2. «Исходные данные для расчета по методике МЭК 61508» предполагает ввод следующих параметров (рис.2):

- интенсивность опасных отказов (λ_d):
- диагностическое покрытие (*DC*), в %.

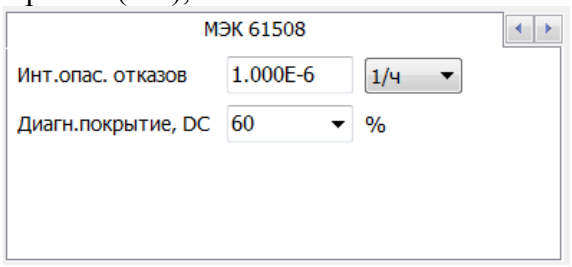


Рисунок 2 – Ввод данных по методике МЭК 61508

Вариант 3. «Исходные данные (ИД) для приближенного расчета» предполагает ввод интенсивности опасных необнаруженных отказов λ_{du} (рис.3).

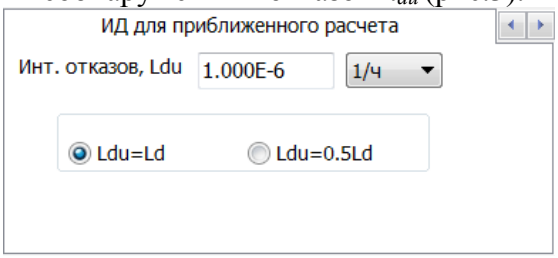


Рисунок 3 – Ввод исходных данных для приближенного расчета

Для приближенных расчетов выбираются два вида предположений:

а) интенсивность опасных необнаруженных отказов λ_{du} равна интенсивности всех опасных отказов. В этом случае параметр *DC*=0%, а доля безопасных отказов (ДБО-SFF) равна 50%;

б) интенсивность опасных необнаруженных отказов λ_{du} составляет 50% от интенсивности опасных отказов λ_D. В это случае параметр *DC*=50%, а ДБО (SFF)= 75%;

Вариант 4. «Неполные ИД».

Неполные исходные включают в себя либо суммарную интенсивность отказов λ, либо среднюю наработку на отказ.

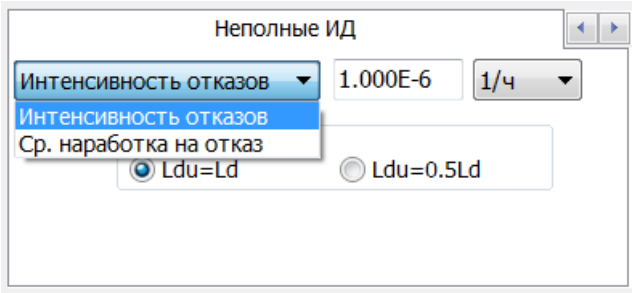


Рисунок 4 – Ввод неполных исходных данных

Расчеты средней вероятности отказа на запрос *PFDavg* может осуществляться при двух предположениях:

а) пессимистическое предположение $\lambda du = \lambda_D$, то есть все опасные отказы не обнаруживаются средствами диагностирования ПАЗ.

В соответствии с данными табл. В1 допускается, что $\lambda_D = 0.5\lambda$.

Тогда

$$PFDavg = \frac{\frac{\lambda}{2}T_1}{2} = \frac{\lambda T_1}{4} \tag{5}$$

является консервативной оценкой показателя ФБ.

б) оптимистическое (инженерное) предположение $\lambda_{du} = 0.5\lambda_D$, то есть система диагностирования обнаруживает 50% опасных отказов.

Тогда

$$PFDavg = \frac{0.5\frac{\lambda}{2}T_1}{2} = \frac{\lambda T_1}{8} \tag{6}$$

является заниженной оценкой показателя ФБ.

Использование упрощенных формул (5) и (6) в инженерных расчетах основано на следующих рассуждениях.

Как был отмечено выше, на практике для определения уровня полноты безопасности используется среднее значение вероятности отказа на запрос *PFD*(t) на межпроверочном интервале T_1

$$PFDavg = \frac{1}{T_1}\int_0^{T_1} PFD(t)dt\ . \tag{7}$$

Выражение (7) может быть записано с использованием вероятности выполнения функции безопасности относительно интенсивности опасных необнаруженных отказов $R(t) = \exp(-\lambda_{du}t)$.

Тогда формула (7) примет вид

$$PFDavg = 1 - \frac{1}{T_1}\int_0^{T_1} \exp(-\lambda_{du}t)dt\ .$$

Используя разложение экспоненциальной функции в ряд Тейлора, после интегрирования получим

$$PFDavg = 1 - \frac{1}{\lambda_{du}T_1}(1 - \exp(-\lambda_{du}T_1)) = 1 - \frac{1}{\lambda_{du}T_1}\left(\lambda_{du}T_1 - \frac{(\lambda_{du}T_1)^2}{2} + ...\right) \approx \frac{\lambda_{du}T_1}{2}\ . \tag{8}$$

Пример 1.

Исходные данные: λd=0.5E-07 (1/ч), MRT=MTTR=8ч.

В табл.3 и 4 приведены сравнительные результаты расчетов показателя *PFDavg* по формуле (1) – столбец ГОСТ, и по формуле (8) при различных значениях межпроверочного интервала T_1.

Таблица 3 – Результаты расчетов показателя *PFDavg* при T_1= 6 месяцев

DC	ГОСТ	Формула (8)	Отн.ошибка, %
0	1.099E-04	1.095E-04	0.36%
60	4.420E-05	4.380E-05	0.90%
90	1.135E-05	1.095E-05	3.52%
99	1.495E-06	1.095E-06	26.76%

Таблица 4 – Результаты расчетов показателя *PFDavg* при T_1= 4 года

DC	ГОСТ	Формула (8)	Отн.ошибка, %
0	8.764E-03	8.760E-03	0.05%
60	3.508E-03	3.504E-03	0.11%
90	8.800E-04	8.760E-04	0.45%
99	9.160E-05	8.760E-05	4.37%

Анализ результатов табл.3 и 4 показывает, что приближенная формула (8) дает заниженный результата оценки показателя *PFDavg* при увеличении доли диагностического охвата (DC). Другими словами, формула (8) не учитывает влияние опасных диагностируемых отказов на показатели функциональной безопасности элемента системы ПАЗ.

Пример 2.

Общая интенсивность отказов элемента ПАЗ λ = 2E-06 1/ч.

1. Предположим, $\lambda du = \lambda_D$ (DC = 0%). Тогда $\lambda_D = \lambda du = 0.5\lambda$ = 1E-06 1/ч.

Если интервал между контрольными проверками (proof test) T_1=8760 час, то

$$PFDavg = \frac{\lambda T_1}{4} = \frac{2E-06 \cdot 8760}{4} = 4.380E-03 .$$

2. Предположим, $\lambda du = 0.5\lambda_D$ (DC = 50%). Тогда $\lambda du = 0.5\lambda_D = 0.25\lambda$ = 0.5E-06 1/ч.

Если интервал между контрольными проверками (proof test) T_1=8760 час, то

$$PFDavg = \frac{\lambda T_1}{8} = \frac{2E-06 \cdot 8760}{8} = 2.198E-03 .$$

Результаты расчетов показывают значительное влияние качества систем диагностирования элементов системы ПАЗ на показатели функциональной безопасности и важности, в частности, реализации процедуры анализа видов и последствий отказов.

3 Модуль для анализа структуры канала ПАЗ

Согласно предположениям стандарта [1] о высокой надежности элементов системы ПАЗ (низких значениях вероятностей отказов на запрос *PFDavg*) процедура расчета для последовательных структур (рис.5) может быть сведена к элементарной операции сложения вероятностей отказов.

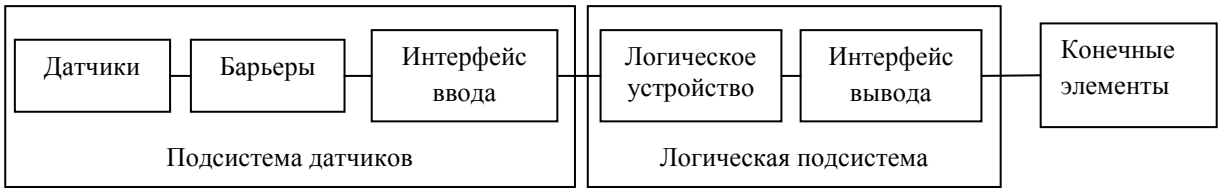


Рисунок 5 – Последовательная структура системы ПАЗ

Для структуры, показанной на рис.5, средняя вероятность отказа на запрос может быть вычислена по формуле

$$PFDsys = PFFED_D + PFD_L + PFD_{FE} =$$
$$= PFD_{Д} + PFD_{Б} + PFD_{ИВ} + PFD_{ЛУ} + PFD_{ИВ} + PFD_{ИМ}' \quad (9)$$

PFDsys – средняя вероятность отказа на запрос системы ПАЗ;
PFD_L – средняя вероятность отказа на запрос логической подсистемы;
PFD_{FE} – средняя вероятность отказа на запрос подсистемы конечных элементов;
$PFD_Д$ – средняя вероятность отказа на запрос датчиков;
$PFD_Б$ – средняя вероятность отказа на запрос искрогасящих барьеров;
$PFD_{ЛУ}$ – средняя вероятность отказа на запрос логического (решающего) устройства;
$PFD_{ИВ}$ – средняя вероятность отказа на запрос интерфейса ввода/вывода;
$PFD_{ИМ}$ – средняя вероятность отказа на запрос исполнительных механизмов.

Согласно рекомендациям п.В.3.2.1 стандарта [1] процедура расчета показателя *PFDavg* включает в себя:

- определение всех элементов, входящих в состав подсистем датчиков, исполнительных механизмов и логической подсистемы;
- представление элементов одной или нескольких голосующих групп 1oo1, 1oo2, 1oo2D, 2oo3, 1oo3;
- расчет показателей *PFDavg* для голосующих групп по формулам (1)–(4);
- средняя вероятность отказа на запрос подсистем и всей системы ПАЗ рассчитывается как сумма *PFDavg* всех элементов.

В соответствии с указанной процедурой в расчетный модуль добавлена страница «Структура канала» (рис.6).

Алгоритм применения расчетного модуля для решения задач анализа показателей функциональной безопасности предполагает следующие шаги:

1 расчет показателя *PFDavg* для элемента структуры канала с использованием одного из вариантов страниц «Расчет вероятности отказа на запрос *PFDavg*»;

2 по управляющей кнопке «Структура канала» перейти на страницу «Расчет параметров элементов канала»;

3 нажатием кнопки «Группа 1» («Группа 2»,…) ввести исходные данные о безотказности элементов, образующих группу (интенсивности обнаруженных опасных отказов *Ldd*, необнаруженных опасных отказов *Ldu*, безопасных обнаруженных отказов *Lsd*);

4 выбрать необходимую архитектуру элемента подсистемы (1oo1, 1oo2, 1oo2D, 2oo3, 1oo3);

5 нажатием кнопки «Расчет 1» («Расчет 2»…) произвести расчет показателя функциональной безопасности элементов групп 1, 2,…;

6. после расчета показателей функциональной безопасности для всех элементов после нажатия кнопки «Сумма по каналу» в соответствующих ячейках отображаются результаты суммирования по интенсивностям отказов (*Ldd*, *Ldu* и *Lsd*), а также по средней вероятности отказа на запрос *PFD* или средней частоты опасных отказов *PFH* канала.

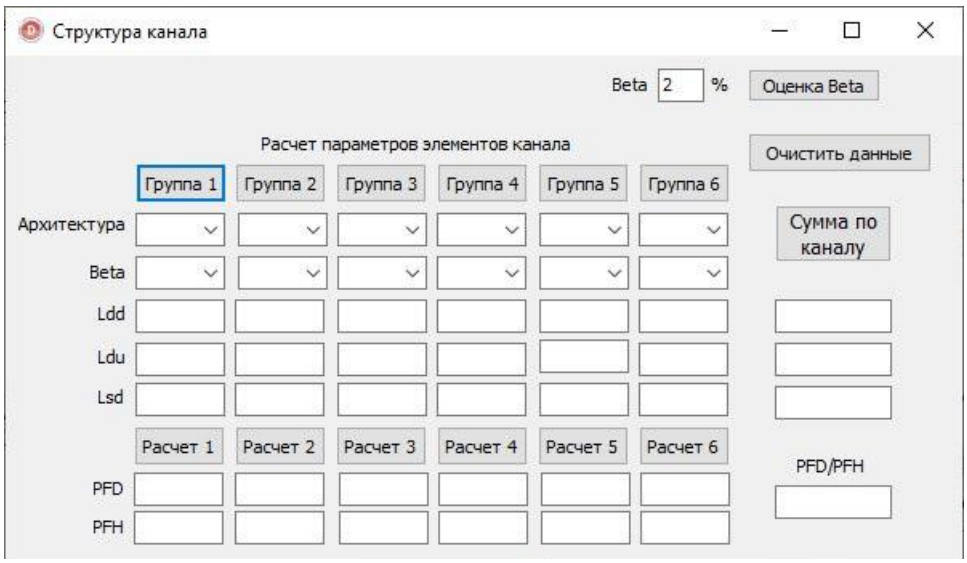


Рисунок 6 – Страница «Структура канала»

Для иллюстрации работы модуля в режиме анализа структуры канала рассмотрим задачу анализа подсистемы датчиков, работающей по логике 2оо3.

Пример 3.

Подсистема датчиков состоит из трех датчиков (Д), трех искрогасящих барьеров (Б) и трех элементов интерфейса ввода (ИВ).

Для всех элементов межпроверочный интервал составляет 1 год.

Показатели ремонтопригодности MTTF=MRT=8час.

Исходные данные о безотказности элементов подсистемы приведены в табл.5.

Предположим, что датчики, барьеры и интерфейсы образуют разные из-за технологий производства и условий эксплуатации группы отказов по общим причинам (ООП) и этим группам соответствуют коэффициенты β-модели 10, 5 и 2% соответственно.

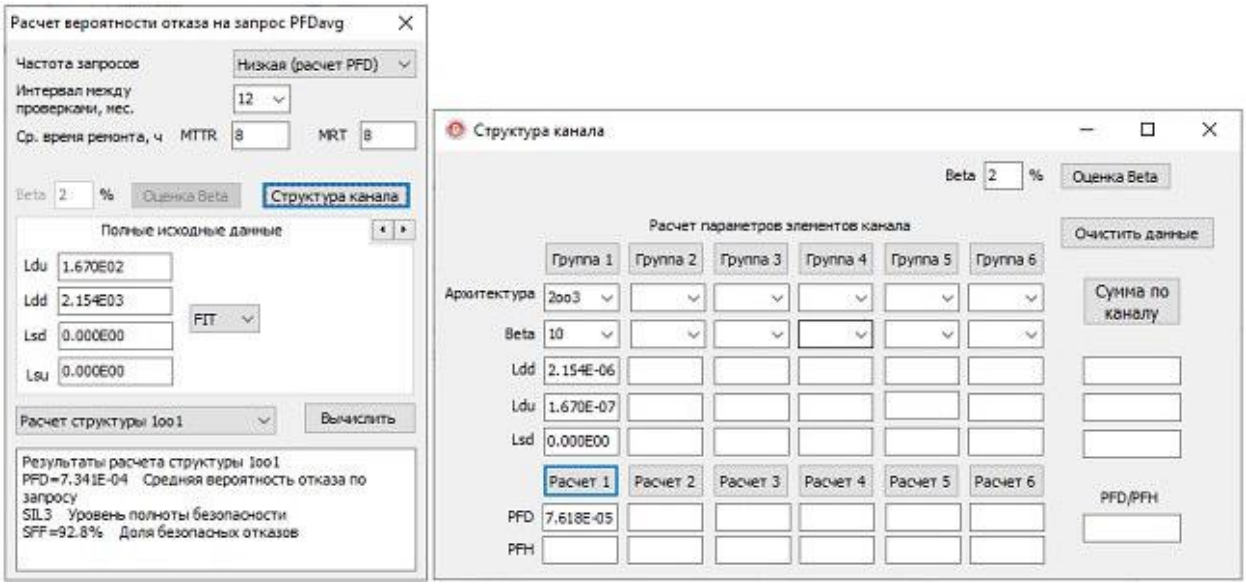
Таблица 5 – Исходные данные о безотказности элементов

Наименование компонента	λdu (FIT)	λdd (FIT)	λsu (FIT)	λsd (FIT)	To (г)
Датчик	167	2154	0	0	-
Искрогасящий барьер	45	-	-	-	-
Интерфейс ввода					150

Расчет показателей функциональной безопасности датчиков.

Шаг 1-2. Для расчета показателя *PFDavg* датчиков применим первую страницу модуля (рис.7а).

Шаг 3-5. После ввода данных о надежности датчиков на страницу «Структура канала» рассчитаем показатель *PFDavg* для голосующей группы 1 по структуре 2оо3 (рис.7б).

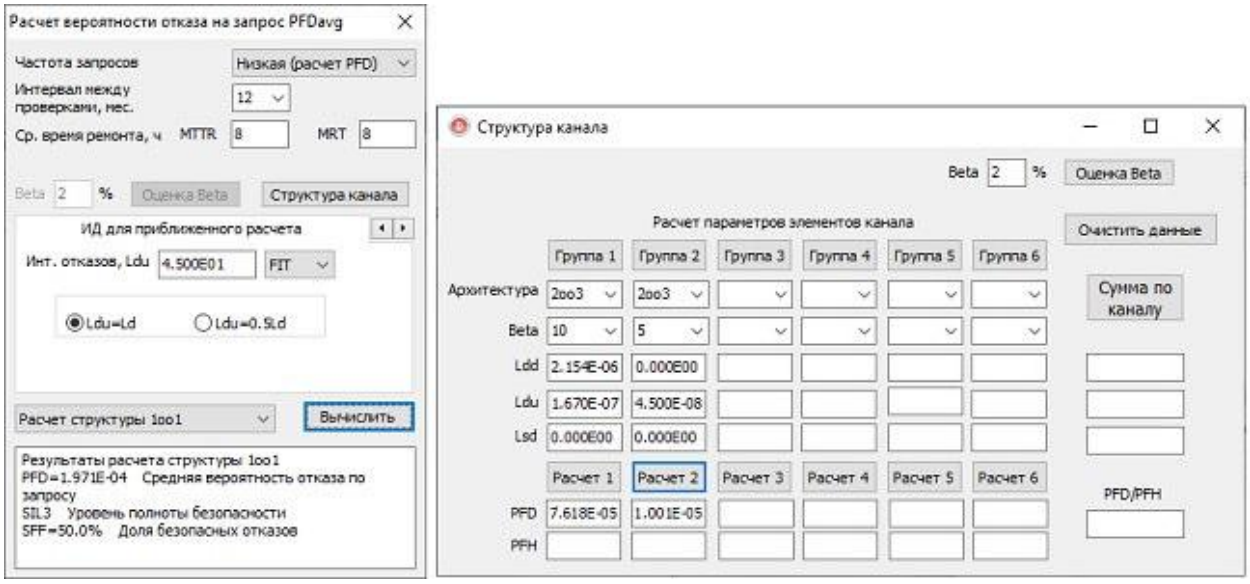


а) б)

Рисунок 7 – Расчет показателя *PFDavg* для датчиков

Расчет показателей функциональной безопасности барьеров.

Шаг 1-2. Для расчета показателя *PFDavg* барьеров применим третью страницу модуля (рис.8а).



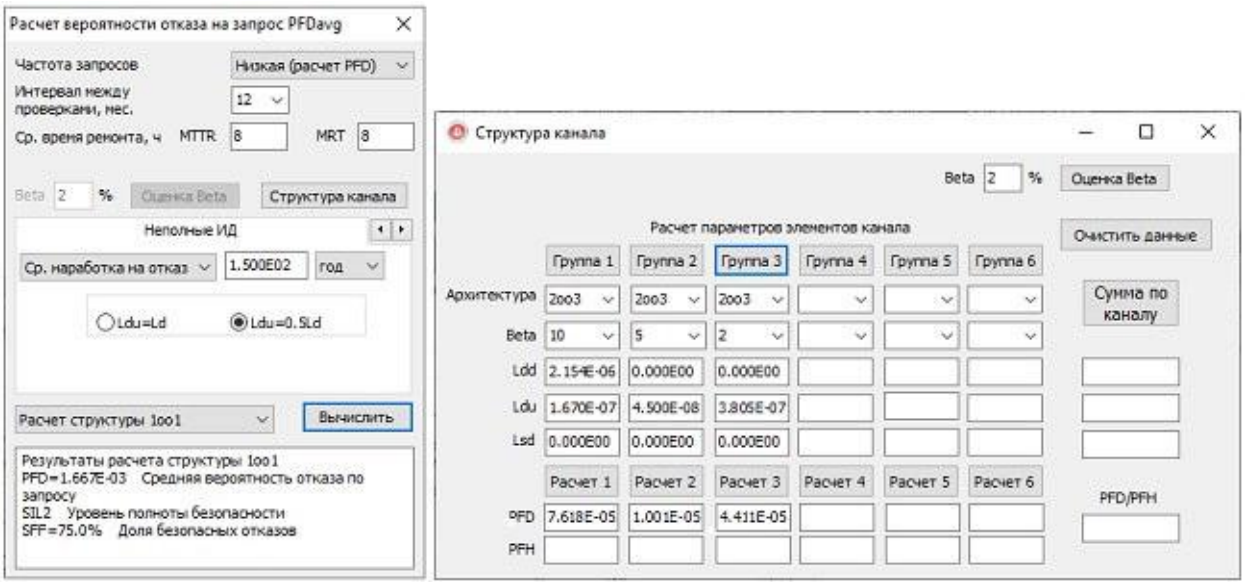
а) б)

Рисунок 8 – Расчет показателя *PFDavg* для барьеров

Шаг 3-5. После ввода данных о надежности барьеров на страницу «Структура канала» рассчитаем показатель *PFDavg* для голосующей группы 2 по структуре 2oo3 (рис.8б).

Расчет показателей функциональной безопасности интерфейсов ввода/вывода.

Шаг 1-2. Для расчета показателя *PFDavg* интерфейсов ввода/вывода применим четвертую страницу модуля (рис.9а).



а) б)

Рисунок 9 – Расчет показателя *PFDavg* для интерфейсов ввода/вывода

Шаг 3-5. После ввода данных о надежности интерфейсов ввода/вывода на страницу «Структура канала» рассчитаем показатель *PFDavg* для голосующей группы 3 по структуре 2oo3 (рис.8б).

Расчет показателя *PFDavg* для всей подсистемы датчиков.

Шаг 6. После нажатия кнопки «Сумма по каналу» в ячейке «PFD/PFH» отображается результат оценки функциональной безопасности подсистемы датчиков (рис.10).

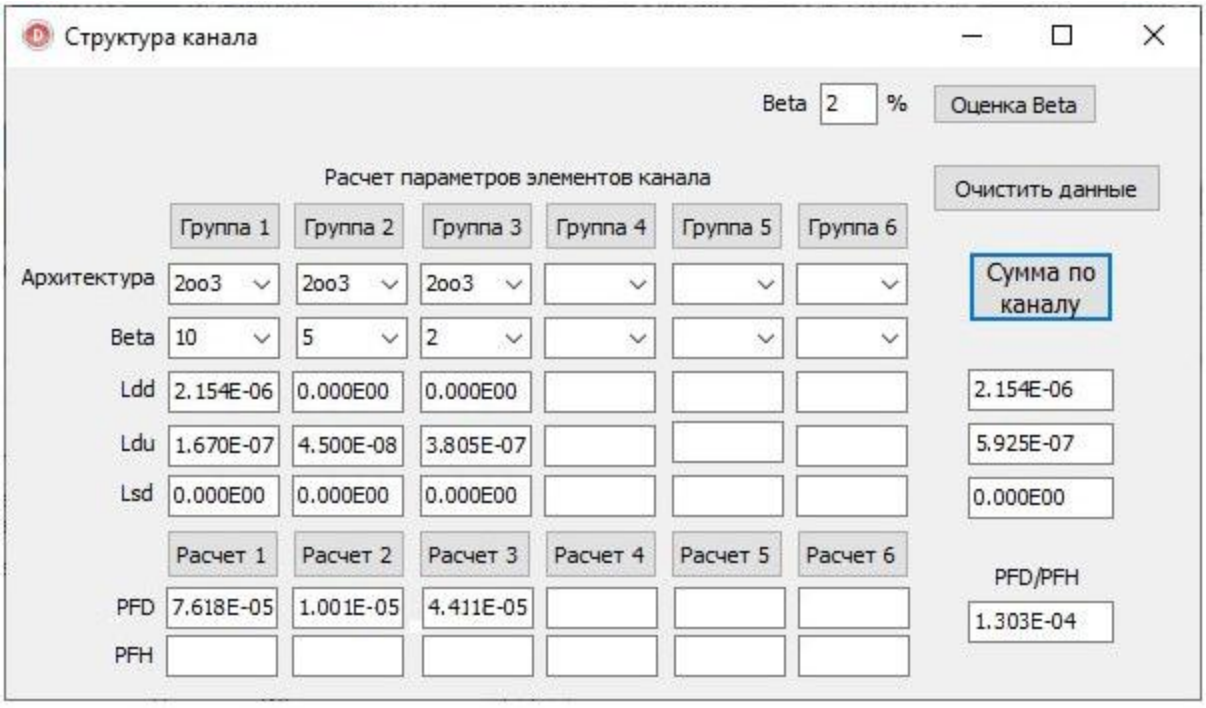


Рисунок 10 – Расчет показателя *PFDavg* всей подсистемы датчиков

3 Структурно-логический метод решение задачи

Как было указано выше, для решения задач оценки функциональной безопасности систем ПАЗ могут использоваться программные продукты, которые должны быть верифицированы на соответствие требованиям стандартов серии МЭК 61508–2012.

Рассмотрим два варианта решения примера 3 с помощью ПК АРБИТР.

Способ 1. Упрощенное дерево неисправностей.

На рис.11 показана схема функциональной целостности (СФЦ) ПК АРБИТР для решения задачи по упрощенной методике без учета реальных соединений элементов подсистемы датчиков.

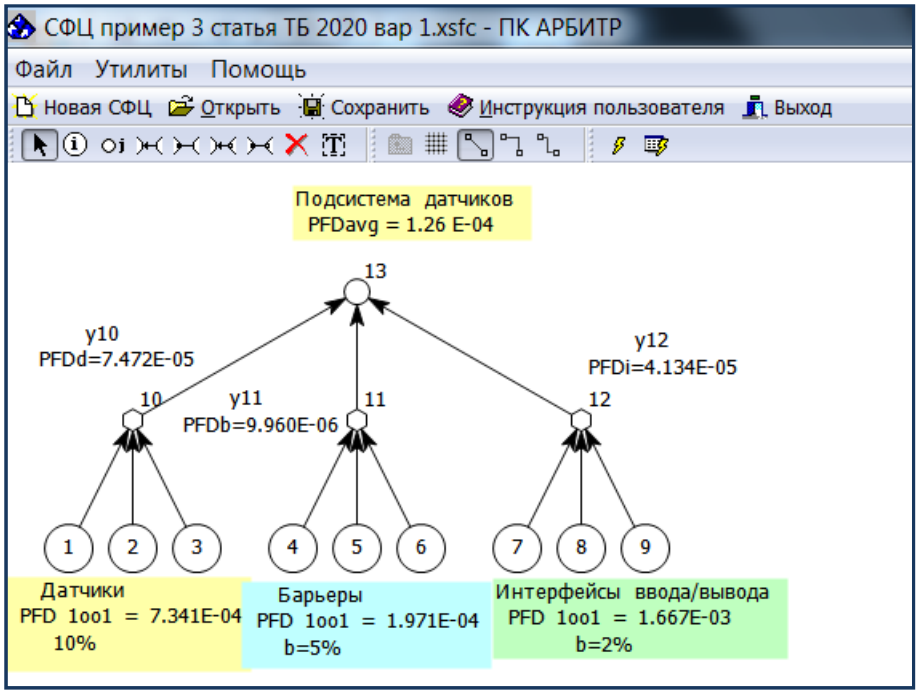


Рисунок 11 – СФЦ для расчета показателя *PFDavg* всей подсистемы датчиков. Вариант1

СФЦ дерева неисправностей на рис.11 состоит из трех дизъюнктивных соединений структур 2oo3 датчиков, барьеров и интерфейсов ввода/вывода. Таким образом данная СФЦ практически повторяет методику модуля, реализованную на странице «Структура канала», с той разницей, что арифметическое сложение заменяет логическое.

В табл. 6 приведены сравнительные результаты описанных выше методов оценки показателя *PFDavg*.

Таблица 6 – Сравнительные результаты методов оценки показателя *PFDavg*

Метод оценки	Датчики	Барьеры	Интерфейсы ввода/вывода	Подсистема датчиков
«Структура канала»	7.618E-05	1.001E-05	4.411E-05	1.303E-04
ПК АРБИТР	7.472E-05	9.960E-06	4.134E-05	1.260E-04

Использование логического подхода при решении задачи оценки показателя *PFDavg* дает несколько заниженный результат за счет использования более точной формулы логического сложения вероятностей отказа на запрос элементов.

Способ 2. Уточненное дерево неисправностей.

На рис.12 показана СФЦ для решения задачи с учетом реальных соединений элементов подсистемы датчиков.

Реальные схемы соединения датчиков, барьеров и интерфейсов ввода/вывода в системах ПАЗ предполагают в основном одноканальные схемы, то есть конкретный датчик соединен с соответствующим барьером, а барьер – с соответствующим интерфейсом ввода/вывода. Граница подсистемы датчиков согласно методике стандарта [1] находится там, где впервые сравниваются сигналы датчиков. Чаще всего это происходит в логическом устройстве (контроллере).

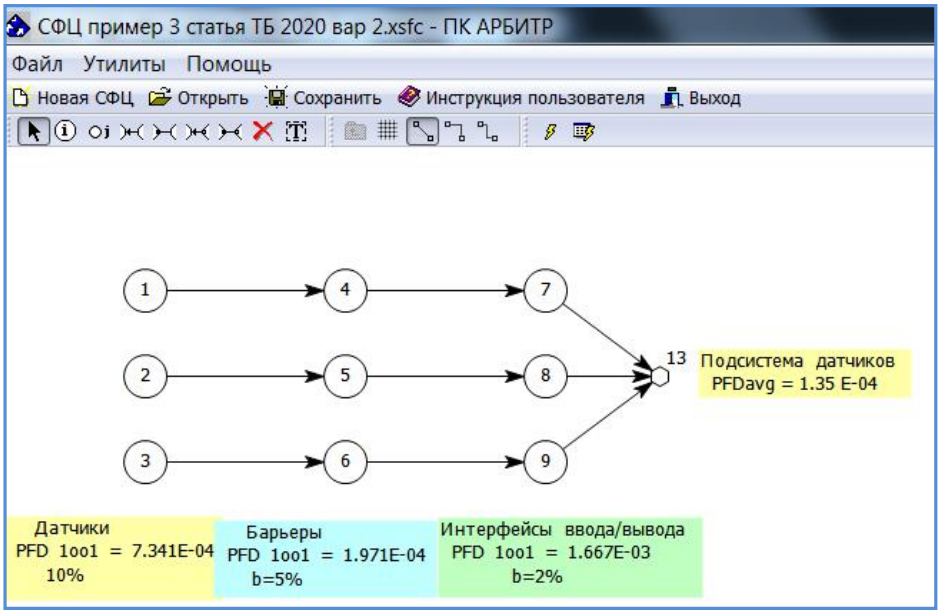


Рисунок 12 – СФЦ для расчета показателя *PFDavg* всей подсистемы датчиков. Вариант 2

Корректность построения СФЦ на рис.12 может быть определена на основе анализа логической функции, фрагмент которой показан в табл.7.

Таблица 7 – Логическая функция для решения примера 3

№ кон.	Ркон.	ЛФ
1	7.341E-5	CCF1[D1,D2,D3]
2	3.334E-5	CCF3[ИВ1,ИВ2,ИВ3]
3	9.855E-6	CCF2[Б1,Б2,Б3]
4	2.668845E-6	ИВ1 ИВ2
5	2.668845E-6	ИВ1 ИВ3
6	2.668845E-6	ИВ2 ИВ3
7	1.07934283E-6	D2 ИВ1
8	1.07934283E-6	D1 ИВ2
9	1.07934283E-6	D1 ИВ3
10	1.07934283E-6	D3 ИВ1
11	1.07934283E-6	D3 ИВ2
12	1.07934283E-6	D2 ИВ3
13	4.36511276E-7	D1 D2
14	4.36511276E-7	D2 D3
15	4.36511276E-7	D1 D3
16	3.05894667E-7	Б1 ИВ3
17	3.05894667E-7	Б1 ИВ2
18	3.05894667E-7	Б2 ИВ1
19	3.05894667E-7	Б3 ИВ1
20	3.05894667E-7	Б2 ИВ3
21	3.05894667E-7	Б3 ИВ2
22	1.23710899E-7	D2 Б1
23	1.23710899E-7	D3 Б1
24	1.23710899E-7	D1 Б2
25	1.23710899E-7	D2 Б3
26	1.23710899E-7	D1 Б3
27	1.23710899E-7	D3 Б2
28	3.506069E-8	Б2 Б3
29	3.506069E-8	Б1 Б3
30	3.506069E-8	Б1 Б2

Логическая функция состоит из 30 конъюнкций и описывает все возможные минимальные сечения отказов элементов, приводящие к отказу подсистемы датчиков.

Следует заметить, что именно такая логическая функция позволяет получить более консервативную оценку показателя *PFDavg*, чем результат по упрощенной методике.

4 Алгоритм решения обратной задачи

В инженерной практике часто требуется сформировать требования по безотказности к элементам системы ПАЗ для обеспечения требуемой полноты безопасности. В стандартах серии МЭК 61511–2018 заданы границы значений показателя *PFDavg*, которые соответствуют уровням полноты безопасности (УПБ-SIL).

Обратной задачей будем считать нахождение значений интенсивности опасных необнаруженных отказов λdu, которая обеспечивает некоторое наперед заданное значение показателя *PFDavg*.

В качестве основы алгоритма решения обратной задачи использованы упрощенные формулы для оценки показателя *PFDavg* для различных структур [6], приведенные в табл.8.

Таблица 8 – Упрощенные формулы для оценки показателя *PFDavg*

Архитектура	Упрощенная формула	Упрощенная формула с β-фактором
1oo2	$\frac{1}{3}\times(\lambda_{DU}\times TI)^2$	$\frac{1}{3}\times[(1-\beta)\times(\lambda_{DU}\times TI)]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
1oo2D	$\frac{1}{3}\times(\lambda_{DU}\times TI)^2$	$\frac{1}{3}\times[(1-\beta)\times(\lambda_{DU}\times TI)]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
2oo2	$\lambda_{DU}\times TI$	$[(1-\beta)\times(\lambda_{DU}\times TI)]+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
2oo3	$(\lambda_{DU}\times TI)^2$	$[(1-\beta)\times(\lambda_{DU}\times TI)]^2+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$
1oo3	$\frac{1}{4}\times(\lambda_{DU}\times TI)^3$	$\frac{1}{4}\times[(1-\beta)\times(\lambda_{DU}\times TI)]^3+\frac{1}{2}\times(\beta\times\lambda_{DU}\times TI)$

На основе данных табл.8 могут быть получены следующие формулы для решения обратной задачи:

для архитектуры 1oo1:

$$\lambda_{du}\cong\frac{2PFD_{1oo1}}{T_1}. \tag{10}$$

Для архитектуры 1oo2 и 1oo2D:

$$\lambda_{du}\cong\frac{-\frac{\beta}{2}+\sqrt{\frac{\beta^2}{4}+4PFDavg\frac{(1-\beta)^2}{3}}}{\frac{2}{3}T_1(1-\beta)^2}. \tag{11}$$

Для архитектуры 2oo3:

$$\lambda_{du}\cong\frac{-\frac{\beta}{2}+\sqrt{\frac{\beta^2}{4}+4PFDavg\frac{(1-\beta)^2}{3}}}{2T_1(1-\beta)^2}. \tag{12}$$

Исходными данными для решения обратной задачи оценки функциональной безопасности системы ПАЗ являются:

- заданная средняя вероятность отказа на запрос *PFDavg sys*;

- межпроверочный интервал TI ;
- распределение надежности по подсистемам системы ПАЗ.

Пример распределения надежности по подсистемам представлен в табл.9.

Таблица 9 – Пример распределения надежности по подсистемам

Подсистемы ПАЗ	Датчики	Логические устройства	Конечные элементы
Доля отказов, %	15	10	75

Алгоритм решения обратной задачи состоит из следующих основных этапов:

1 Определяются требования к показателю *PFDavg* каждой подсистемы на основе заданной системной характеристики *PFDavg sys*;

2 В зависимости от выбранной архитектуры подсистемы по формулам (10)–(12) рассчитываются значения интенсивности опасных необнаруженных отказов λdu.

3 Проверка полученных результатов выполняется с использованием вычислительного модуля.

В настоящее время алгоритм решения обратной задачи реализован в программной среде Excel. Планируется при определенной доработке алгоритма и формировании базы данных о стоимости компонентов системы ПАЗ разработать дополнительную страницу в вычислительном модуле для решения обратной задачи с учетом технико-экономических показателей.

ЛИТЕРАТУРА

1 ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. 2012. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р 61508-3.

2 А.С. Можаев. 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.

3 URL: https://www.isograph.com/software/reliability-workbench/ (Дата обращения 14.05.2019).

4 И.А. Можаева, А.А. Нозик, А.В. Струков. Типовые примеры расчета функциональной безопасности систем противоаварийной защиты опасных производственных объектов // Сборник трудов двадцатой Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности» том 2, «Средства противодействия терроризму», ФБГУ РАРАН-Москва, НПО СМ - СПб., 2019, С.486–494.

5 К.А. Ветлугин, И.А. Можаева, 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.

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