СПИК СЗМА

Проектная оценка функциональной безопасности систем ПАЗ

г. Санкт-Петербург

СПИК СЗМА

Нормативные требования по ФБ систем ПАЗ

ФНиП «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» (ОПВБ)

п. 2.1

Технологические процессы и применяемое технологическое оборудование, **выбор средств** контроля, управления и **ПАЗ должны быть обоснованы в проектной документации результатами анализа опасностей технологических процессов … с использованием методов анализа риска аварий на ОПО**

п. 6.3.4

Системы ПАЗ для объектов, имеющих в своем составе блоки I и II категорий взрывоопасности должны создаваться **на базе логических контроллеров**, способных функционировать по отказобезопасной структуре и **проверенных на соответствие требованиям функциональной безопасности систем электрических, электронных, программируемых электронных связанных с безопасностью**

п. 6.3.5

Методы создания систем ПАЗ должны определяться на стадии формирования требований при проектировании АСУ ТП **на основании анализа** опасности и **работоспособности контуров безопасности с учетом риска, возникающего при отказе контура безопасности**. Рациональный выбор средств для систем ПАЗ осуществляется с учетом их надежности, быстродействия в соответствии с их техническими характеристиками

ГОСТ Р 51901.11 – 2005 (МЭК 61882:2001)
«Исследование опасности и работоспособности (HAZOP)»

ГОСТ Р МЭК 61508 – 2012
«Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»

ГОСТ Р МЭК 61511 – 2016
«Безопасность функциональная. Системы безопасности приборные для промышленных процессов»

Типовые требования ООО «КИНЕФ» на проектирование

1. Состав и содержание работ по проектированию

1.1 Исполнитель проекта должен выполнить следующие работы:

1.1.7 Для подтверждения соответствия требованиям функциональной безопасности систем ПАЗ **предоставить документ «Проектная оценка функциональной безопасности»**, в котором должны быть **определены значения показателей функциональной безопасности** разработанной системы ПАЗ (согласно ГОСТ Р МЭК 61508-6-2012) и **обосновано их соответствие требуемым уровням полноты безопасности УПБ (SIL)** системы ПАЗ (согласно ГОСТ Р МЭК 61511-1-2011). При этом выбор структуры и состава комплекса программно-технических средств, датчиков и исполнительных механизмов системы ПАЗ должен производиться на основании требуемых уровней полноты безопасности УПБ (SIL) функций ПАЗ согласно ГОСТ Р МЭК 61511-1-2011.

Формирование требований на проектирование систем ПАЗ на основании процедуры HAZOP

СПИК СЗМА

1 → **2** → **3**

Анализ опасностей и работоспособности (HAZOP)

ГОСТ Р 51901.11-2005

Определение функций приборной системы безопасности (системы ПАЗ)

ГОСТ Р МЭК 61511-1
ГОСТ Р МЭК 61511-2

Назначение уровней полноты безопасности УПБ

ГОСТ Р МЭК 61511-3

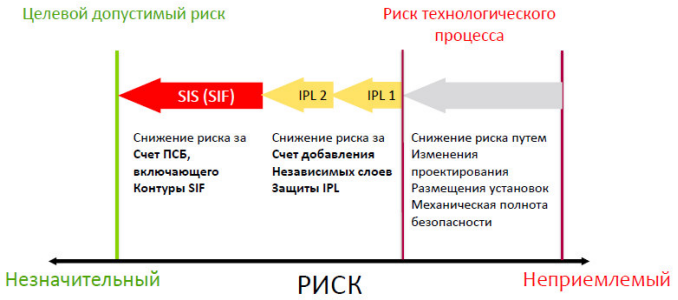
Заголовок исследования: НЕФТЯНОЙ ИСПАРИТЕЛЬ

Рисунок №: | Пересмотр (номер): | Дата:

Состав группы: MG, NE, DH, EK, LB | Дата заседания:

Рассматриваемая часть: ЗМЕЕВИК ИСПАРИТЕЛЯ ОТ ВХОДНОГО ОТВЕРСТИЯ ПОДАЧИ НЕФТИ (ДО ИЗМЕРЕНИЯ ПОТОКА) ДО МЕСТА ВЫХОДА ПАРА (ПОСЛЕ КОНТРОЛЯ ТЕМПЕРАТУРЫ) | Цель проекта: ВХОДЫ: НЕФТЯНОЙ ПОТОК, НАГРЕТЫЙ ПЕЧЬЮ Действия: ИСПАРЕНИЕ, НАГРЕВ И ПОДАЧА НЕФТЯНОГО ПАРА НА ПРОЦЕСС

Порядковый номер	Управляющее слово	Элемент	Отклонение	Возможные причины отклонения	Последствия	Существующие меры безопасности	Примечание	Требуемые действия	Фамилия ответственного за выполнение действий
1	НЕТ	Поток нефти	Нет потока нефти	Отказ поставки нефти. Клапан управления потоком *FCV* закрыт	Змеевик испарителя перегревается и может отказать	Сигнал низкого потока *FAL*. Высокотемпературное реле *TSH*	Безопасность зависит от быстроты реакции оператора	Рассмотреть возможность использования элемента *FE* для перекрывания главного клапана горелки	LB
				Закупоривание змеевика. Блокировка находящего потока испарителя	Заклинание нефти в испарителе. Возможное перегревание и закоксовывание змеевика	Сигнал низкого потока *FAL*. Высокотемпературное реле *TSH*	—	Проверить, являются ли меры безопасности адекватными и легко ли очистить змеевик	NE
2	НЕТ	Нагревание	Нет нагрева	Пламя вне печи	Невыпаренная жидкая нефть подается на процесс	—	—	Исследовать воздействие жидкой нефти на процесс. Обеспечить остановку печи по сигналу выходящего пламени с закрытым *FCV*. Обеспечить подачу сигнала при низкой температуре нефти на выходе	DH
3	БОЛЬШЕ	Поток нефти больше, чем необходимо	Количество тепла в печи больше, чем необходимо	Нефть поступает с более высоким давлением. Отказ контроллера потока *FC*. Неправильно выбрана точка размещения *FC*	Возможна перегрузка испарителя, приводящая к недостаточному нагреванию потока нефти (см. пункт 6)	Нет	—	Проверить способность *FCV* управлять потоком нефти с более высоким давлением. Обеспечить подачу сигнала при низкой температуре нефти на выходе	MG



Перечень контуров ПАЗ с назначенными уровнями полноты безопасности – обязательная часть технического задания (технических требований) на систему ПАЗ

Перечень функций безопасности системы ПАЗ

СПИК СЗМА

Перечень функций безопасности системы ПАЗ паровых котлов высокого давления входящих в состав установки полиэтилена ООО «Новоуренгойский газохимический комплекс»

№ п.п	Функция безопасности ПСБ	Обозначение позиции КИП	Установленный УПБ
1	Блокировка по падению уровня	LZA77311, LZA77312, LZA7731	2
2	Сигнализация роста давления	PIA 77413	1
3	Сигнализация роста давления	PICA 77418	1
4	Сигнализация низкого содержания O_2 и блокировка горелок	QSA77520	1
5	Сигнализация и блокировка по погасанию пламени горелок	XZA77756, XZA77761, XZA77763, XZA77765	2
6	Сигнализация положения шибера и блокировка горелок	GOSA77226, GOSA77227, GOSA77228	2
7	Сигнализация и блокировка по росту давления в топочном пространстве	PZA77421.1, PZA77421.2, PZA77421.3	2
8	Сигнализация и блокировка по падению давления воздуха	PZA77458, PZA77459, PZA77460	2
9	Сигнализация падения давления газа и блокировка горелки	PZA77451, PZA77452, PZA77453	2
10	Сигнализация падения давления газа и блокировка горелки	PZA77262.1, PZA77292.1, PZA77322.1, PZA77352.1	1
11	Сигнализация роста давления газа	PIA77474	1
12	Сигнализация роста давления газа и блокировка горелки	PZA77454, PZA77455, PZA77456	2

Требования к показателям ФБ контура безопасности

1. Требования к отказоустойчивости (структурные ограничения)

УПБ	Минимальное допустимое число отказов		
	60% < ДБО	60% ≤ ДБО ≤ 90%	ДБО > 90%
1	1	**0**	0
2	2	**1**	0
3	3	**2**	1
4	Применяются специальные требования (см. МЭК 61508)		

ГОСТ Р МЭК 61511 – 2011

УПБ	Мин. допустимое число отказов
1	**0**
2 (редкие запросы)	**0**
2 (частые или непрерывные запросы)	**1**
3	**1**
4	**2**
2	1oo3

ГОСТ Р МЭК 61511 – 2016

2. Требования к надежности функционирования контура безопасности

Уровень полноты безопасности	Целевое сокращение риска	Средняя вероятность отказа выполнения по запросу (PFDavg)	Средняя частота отказов в час (PFH)
УПБ 1	$10 - 100$	$10^{-2} - 10^{-1}$	$10^{-6} - 10^{-5}$
УПБ 2	$100 - 1,000$	$10^{-3} - 10^{-2}$	$10^{-7} - 10^{-6}$
УПБ 3	$1,000 - 10,000$	$10^{-4} - 10^{-3}$	$10^{-8} - 10^{-7}$
УПБ 4	$10,000 - 100,000$	$10^{-5} - 10^{-4}$	$10^{-9} - 10^{-8}$

3. требования к мерам по предотвращению систематических отказов

СПИК СЗМА

Исходные данные для расчета вероятности отказа на запрос для контуров ПАЗ

1. Структура контура безопасности

Определяется в соответствии с требования по допустимому количеству отказов согласно заданному уровню полноты безопасности

2. Величины интенсивностей отказов оборудования, входящего в контур

Предоставляются производителями

3. Интервал времени между контрольными проверками оборудования контура

Значения определяются Заказчиком

4. Время восстановления (замены) отказавшего оборудования

Значения определяются Заказчиком

В типовых требованиях, в разделе относящемся к разработке систем ПАЗ, должны быть указаны временные интервалы:

- **проверок технических средств системы ПАЗ;**
- **восстановления (замены) отказавшего оборудования.**

Исходные данные для расчета вероятности отказа на запрос для контуров ПАЗ

1. Структура контура безопасности

2. Количественные величины частот отказов оборудования, входящего в контур

3. Интервал между контрольными проверками оборудования контура

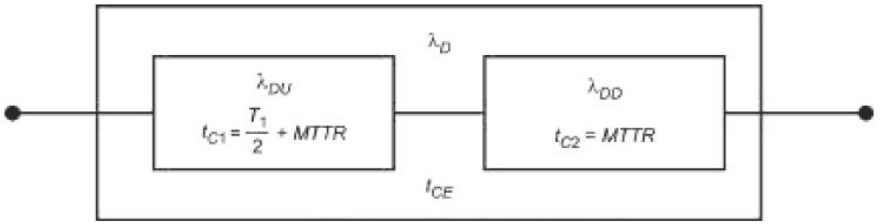
4. Время восстановления (замены) отказавшего оборудования

Структура контура безопасности

СПИК СЗМА

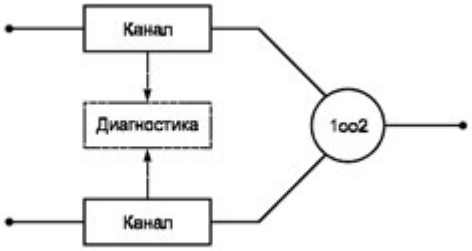
Архитектурные ограничения определяются назначенным уровнем УПБ для данной функции безопасности

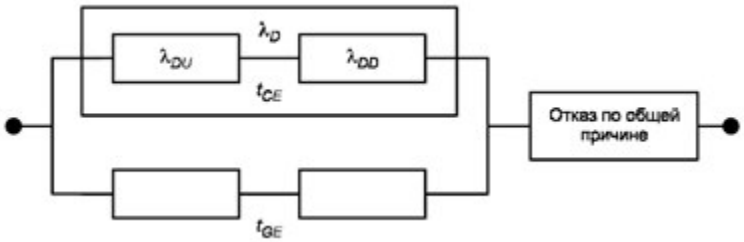
Структура 1oo1



$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \qquad PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Структура 1oo2





$$\lambda_{DU} = \frac{\lambda}{2}(1-DC);\ \lambda_{DD} = \frac{\lambda}{2} DC \qquad t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \qquad t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

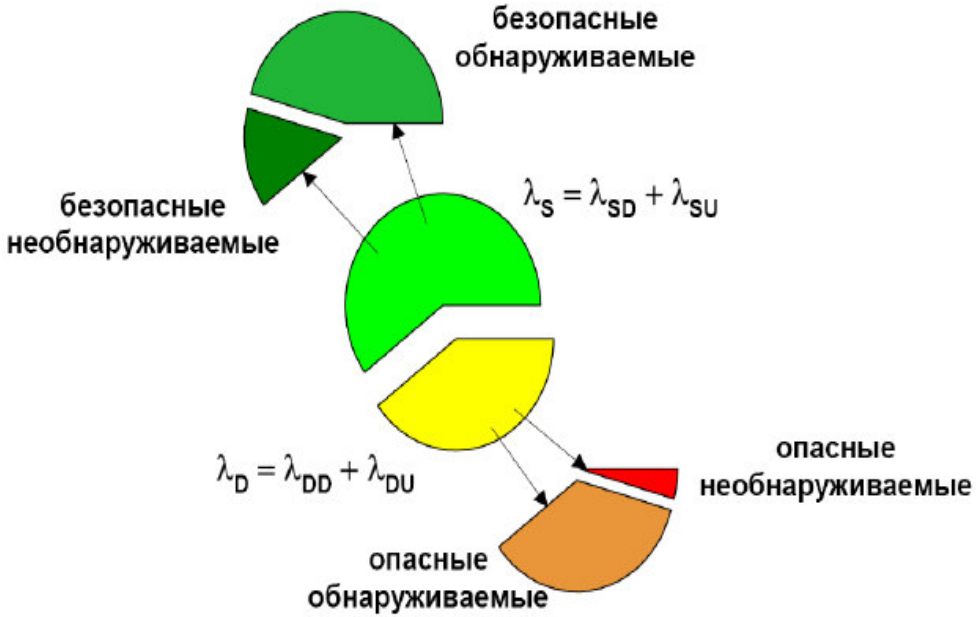
Исходные данные для расчета вероятности отказа на запрос для контуров ПАЗ

1. Структура контура безопасности
2. Количественные величины частот отказов оборудования, входящего в контур
3. Интервал между контрольными проверками оборудования контура
4. Время восстановления (замены) отказавшего оборудования

Структура частоты отказов

СПИК СЗМА

$$\lambda_{Total} = \lambda_S + \lambda_D$$



$$ДБО = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} = 1 - \frac{\lambda_{DU}}{\lambda_{Total}}$$

(ГОСТ 61508-4)

Опасный отказ:

- препятствует выполнению ФБ, переводя УО в **опасное состояние**
- **снижает вероятность** корректного **выполнения** ФБ

Безопасный отказ:

- **приводит к ложному выполнению** ФБ, переводящее УО в **безопасное состояние**
- **увеличивает вероятность ложного выполнения** ФБ

Необнаруженный отказ:

- не установленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора

Обнаруженный отказ:

- установленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора

Количественные величины частот отказов оборудования

1 На сайте производителя

Руководство по безопасности

Safety Manual
VEGAFLEX series 60
4 … 20 mA/HART two-wire
4 … 20 mA/HART four-wire

Document ID:
31339

Guided Microwave

Failure rates

Applies to overfill and dry run protection:

λ_{sd}	0 FIT
λ_{su}	343 FIT
λ_{dd}	990 FIT
λ_{du}	203 FIT
DC_S	0 %
MTBF = MTTF + MTTR	0.54×10^6 h

Specific characteristics

Single channel architecture (1oo1D)

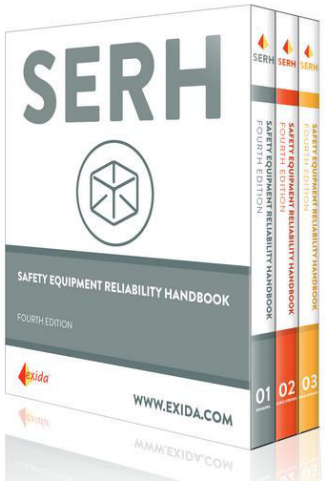
SIL	SIL2
HFT	0
Sensor type	Type B

Applies to overfill and dry run protection:

SFF	86 %
PFD_{avg} T_{Proof} = 1 year T_{Proof} = 5 years	 $< 0.089 \times 10^{-2}$ $< 0.443 \times 10^{-2}$
PFH	$< 0.203 \times 10^{-6}$/h

Количественные величины частот отказов оборудования

2 Специальные справочники



Safety Equipment Reliability Handbook - 4th Edition

3 Данные по надежности

Выбор компонентов на основе опыта их предшествующего применения

Известна только наработка на отказ, требуется предположение о распределение отказов по типам, например:

$$\lambda_S = \lambda_D = \frac{\lambda_{Tot}}{2}$$

$$\lambda_{DU} = \lambda_{DD} = \frac{\lambda_D}{2}$$

Исходные данные для расчета вероятности отказа на запрос для контуров ПАЗ

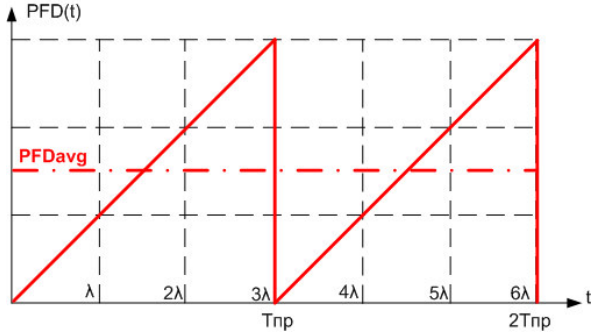
1. Структура контура безопасности

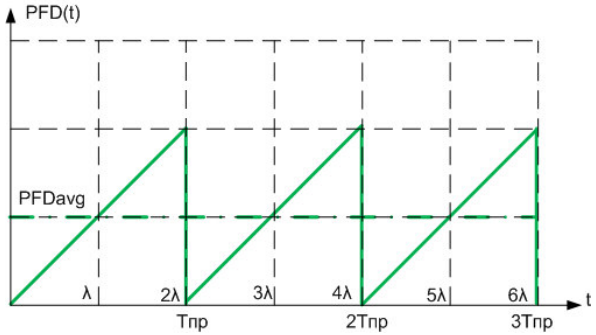
2. Количественные величины частот отказов оборудования, входящего в контур

3. Интервал между контрольными проверками оборудования контура

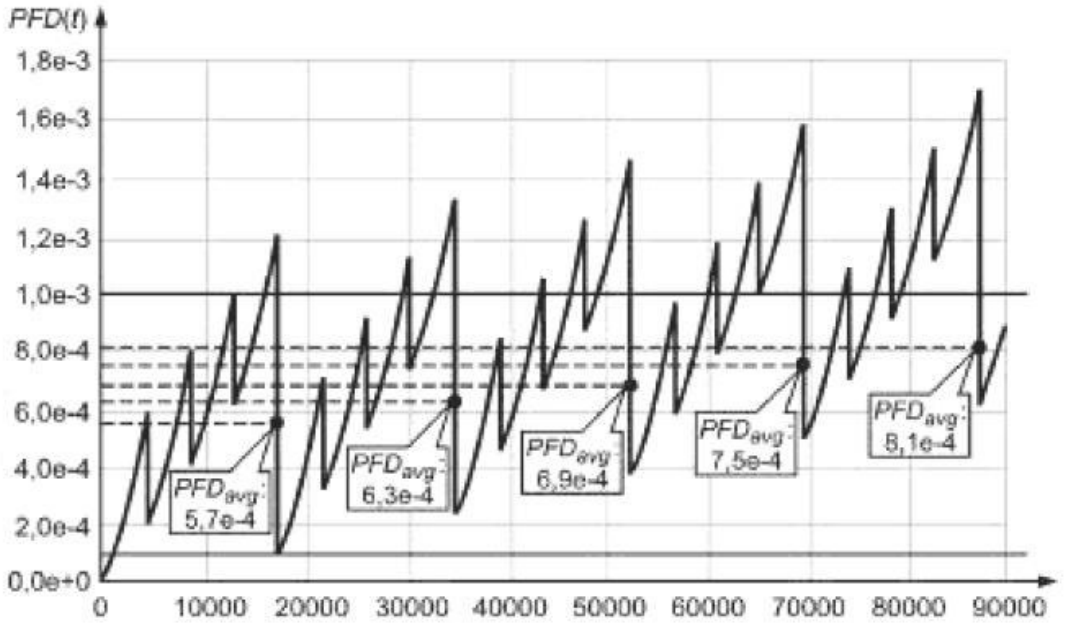
4. Время восстановления (замены) отказавшего оборудования

Интервал между контрольными проверками оборудования контура





С уменьшением интервал между контрольными проверками уменьшается PFDavg



Если некоторые элементы не проверяются, то PFDavg растет со временем

Методика расчета средней вероятности отказа на запрос для контуров системы ПАЗ

СПИК СЗМА

1. Основные термины и определения

2. Общие положения

2.1 Методы и подходы

2.2 Допущения

2.3 Содержание методики

2.3.1 Формирование исходных данных

2.3.2. Расчет вероятностей отказа на запрос элементов с помощью утилиты

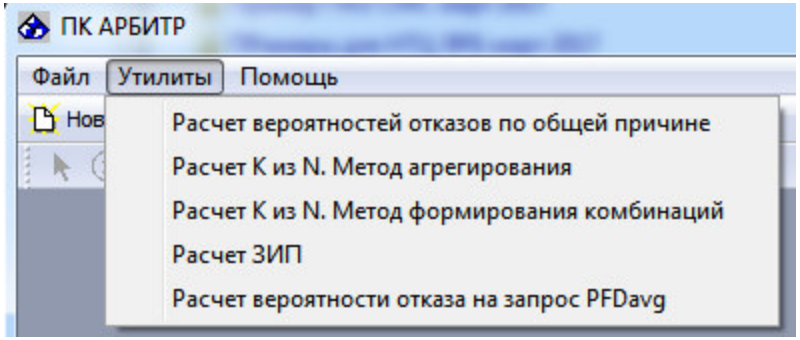
2.3.3. Оценка вероятности отказа на запрос контуров безопасности ПАЗ с применением ПК АРБИТР

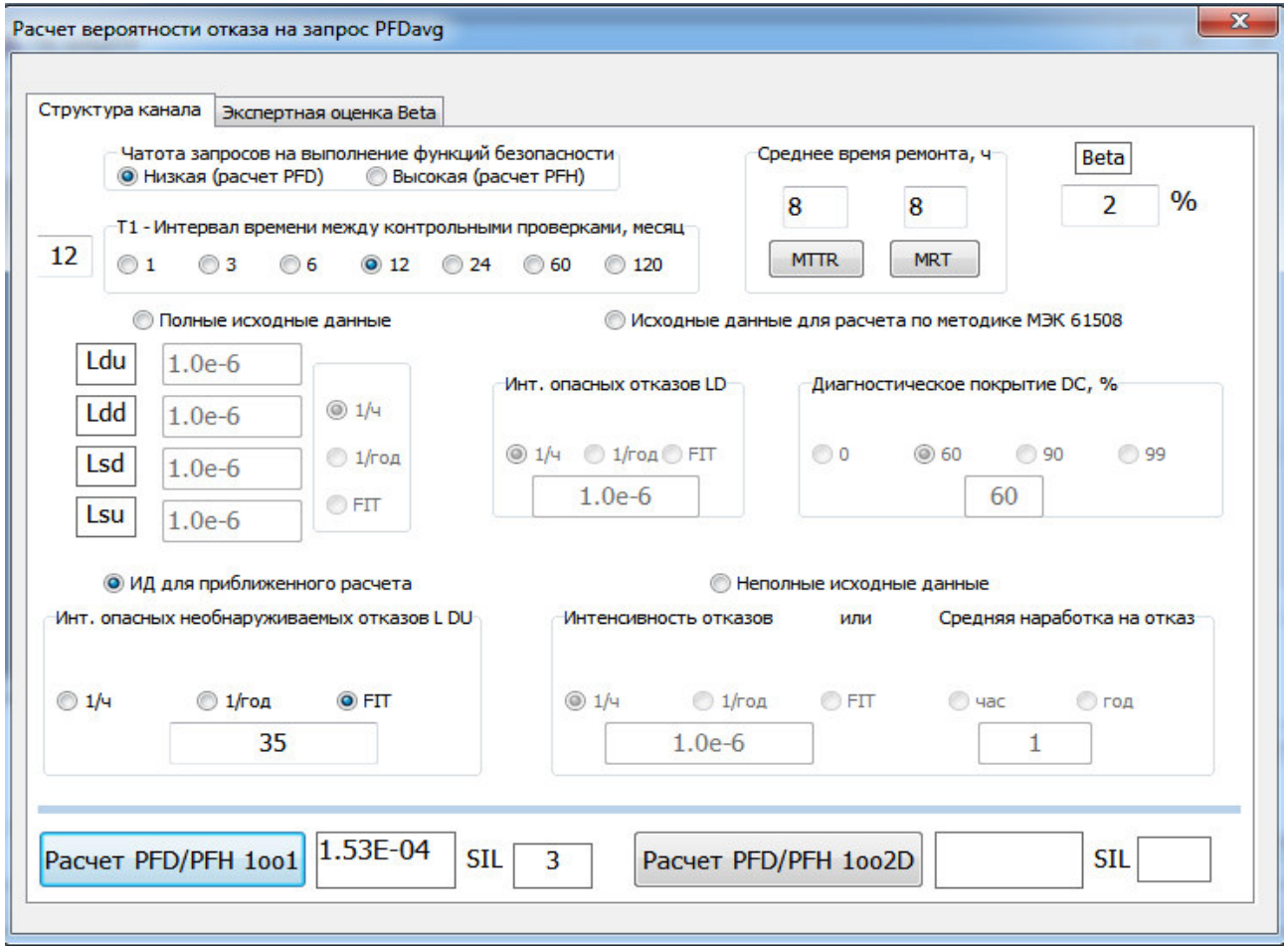
Методика апробирована при расчетах примеров контуров содержащихся в стандартах ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61511-2.

Подтверждена идентичность расчетов ПК АРБИТР методикам приведенным в стандартах ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61511-2.

Утилита для расчета PFD для элементов контра ПАЗ

СПИК СЗМА

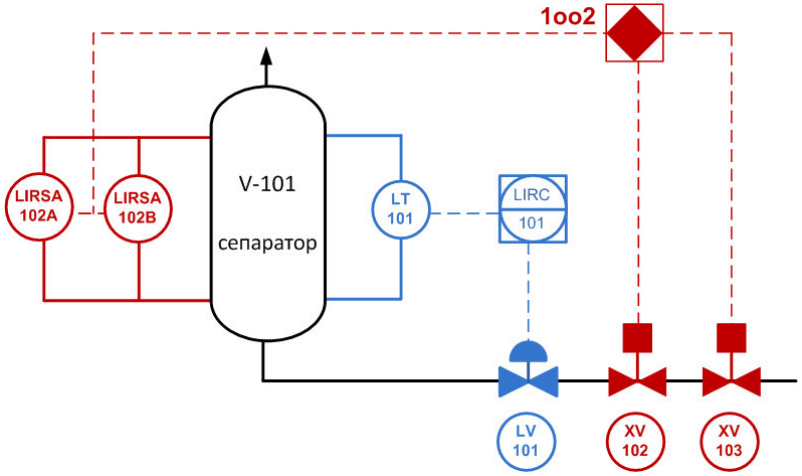


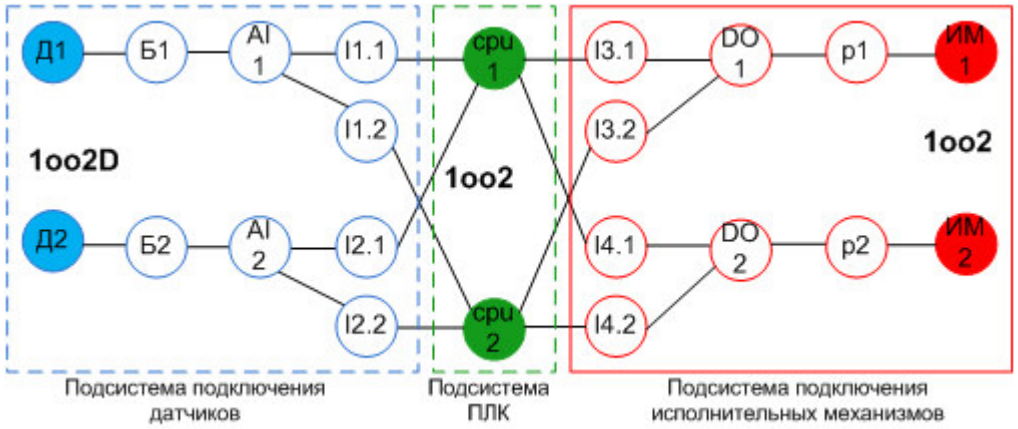


Пример. Подтверждение УПБ (SIL) контуров ПАЗ

СПИК СЗМА

Функция безопасности: защита от превышения предельно-допустимого значения уровня в сепараторе газа для горелок котлов высокого давления.
При обнаружении превышения предельно-допустимого значения уровня в сепараторе перекрыть поток на входе в сепаратор.
Назначенный уровень полноты безопасности – **УПБ 3**.





Обозначение	Элемент	Производитель
Д1, Д2	Датчик уровня VEGAFLEX 61	VEGA
Б1, Б2	Барьер MTL 4541B	MTL
AI1, AI2	Модуль AI SM336F	Siemens
I1.1 – I4.1	Интерфейсный модуль	Siemens
CPU1, CPU2	Контроллер 417-4FH	Siemens
DO1, DO2	Модуль DO SM326F	Siemens
P1, P2	Релейный модуль D5019S	GM
ИМ1, ИМ2	Привод AUMA SAEx2 с AMExC.1	Auma

Пример. Исходные данные

СПИК СЗМА

Исходные данные для расчета PFD подсистемы подключения датчиков

Обозначение	№ СФЦ	Элемент	Производитель	Lsu (FIT)	Ldd (FIT)	Ldu (FIT)	MTBF (г)
D1, D2	1, 6	Датчик уровня	**VEGA**	**343**	**990**	**203**	61.6
Б1, Б2	2, 7	Барьер	**MTL**	**116**	**210**	**17**	
AI-1, AI-2	3, 8	Модуль AI	**Siemens**	3880	301	129	**26.5**
I1.1-I2.2	4,5,9,10	Интерф.модуль	**Siemens**	733	209	104	**106**

Исходные данные для расчета PFD подсистемы ПЛК

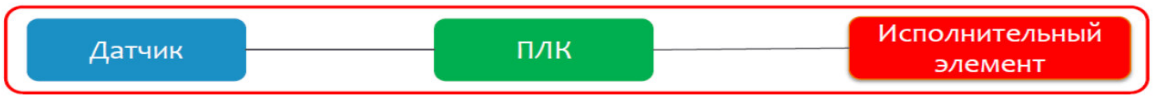
Обозначение	№ СФЦ	Элемент	Производитель	Lsu (FIT)	Ldd (FIT)	Ldu (FIT)	MTBF (г)	PFD (4 года)
CPU1,CPU2	11, 12	ПЛК	**Siemens**					**1.02E-04**

Исходные данные для расчета PFD подсистемы подключения ИМ

Обозначение	№ СФЦ	Элемент	Производитель	Lsu (FIT)	Ldd (FIT)	Ldu (FIT)	MTBF (г)
D01, D02	15, 20	Модуль DO	**Siemens**	3039	236	101	**33.8**
P1, P2	16, 21	Релейный модуль	**GM**	96	3.64		
ИМ1, ИМ2	17, 22	Привод	**Auma**	808	367	647	
I3.1-I4.2	13,14, 18,19	Интерф.модуль	**Siemens**	733	209	104	**106**

Пример. Расчет вероятности отказа на запрос

СПИК СЗМА

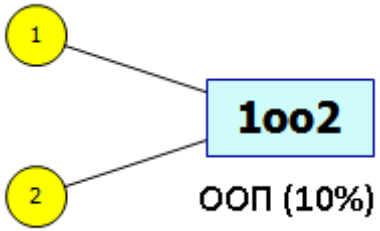


$$PFD_{контур} \approx PFD_{датчик} + PFD_{ПЛК} + PFD_{ИсполЭлемент}$$

S7-300/400 F-CPUs	Article number	Operation in low demand mode low demand mode (PFD = average probability of failure on demand)	Operation in high demand or continuous mode high demand/continuous mode (PFH = probability of a dangerous failure per hour)	With a mission time of	S	D	F
CPU 417-4H	6ES7417-4HL04-0AB0	< 1.9E-04 < 3.8E-04	< 4.3E-09 < 4.3E-09	10 years 20 years	-	-	x
	6ES7417-4HT14-0AB0	< 1.9E-04 < 3.8E-04	< 4.3E-09 < 4.3E-09	10 years 20 years	-	-	x

PFDavg and PFH values for components with use in SIMATIC Safety, Distributed Safety and F/FH Systems
A5E03310062-AE, 10/2015

Логическая подсистема (архитектура 1oo2)

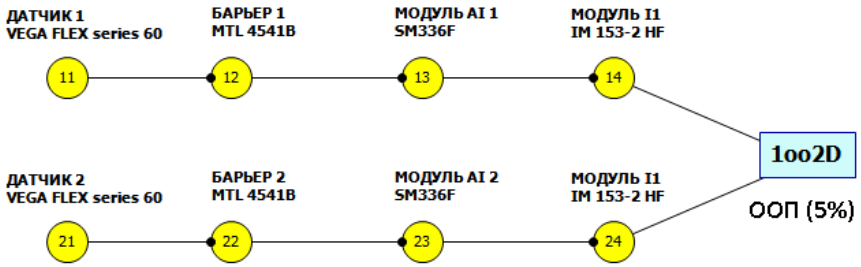


T, год	T proof, год (PLC)	PFDavg
1	-	1,9E-06
2	-	3,8E-06
3	-	5,7E-06
4	-	7,6E-06

Пример. Расчет вероятности отказа на запрос

СПИК СЗМА

Подсистема датчиков (архитектура 1oo2D)

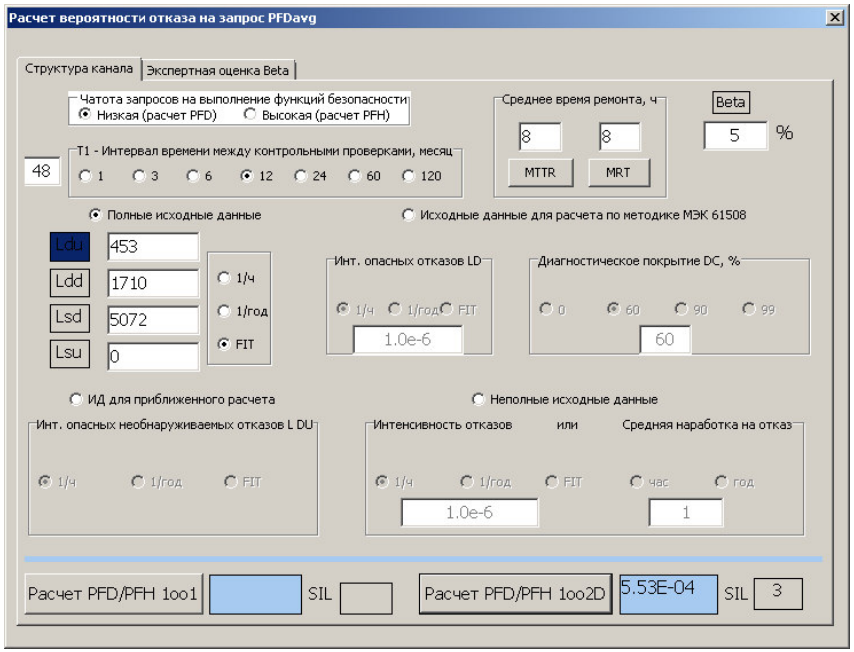


Суммарные интенсивности отказов канала

Lsd=5072 FIT Ldu=453 FIT Ldd=1710 FIT

Использование утилиты для расчета структуры 1oo2D (с учет ООП (5%) и интервала между проверками)

Расчет PFD для структуры 1oo2D с помощью утилиты



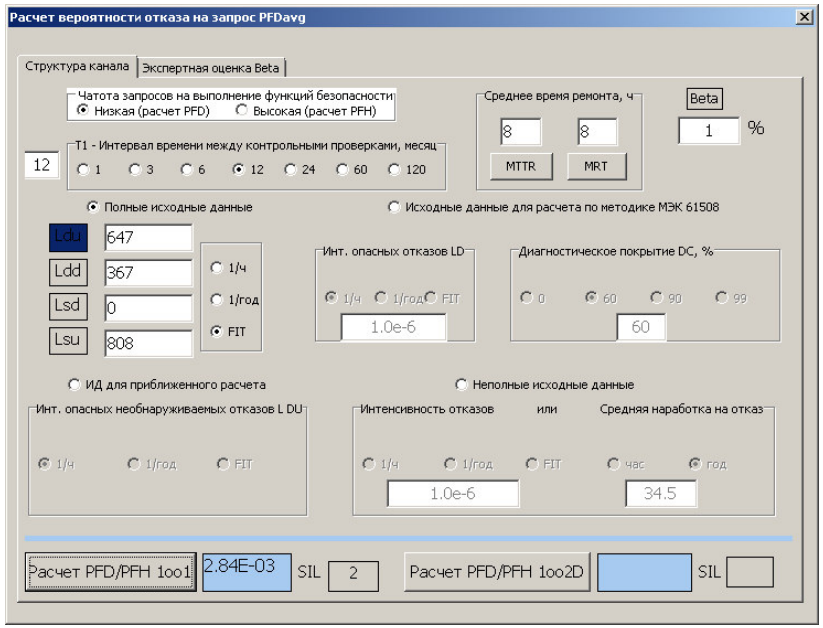
T, год	T proof, год (датчики)	PFDavg
4	4	5,53E-04
4	1	3,33E-04
4	0,5	3,00E-04

Пример. Расчет вероятности отказа на запрос

СПИК СЗМА

Подсистема исполнительных элементов (архитектура 1oo2)

Ввод исходных данных для расчета PFD клапана



T, год	T proof, год	PFDavg
1	-	3,05E-04
2	-	6,20E-04
3	-	9,46E-04
4	-	1,28E-03

Для структуры подсистемы исполнительных элементов (1oo1), работа 4 года, проверка раз в 1 год

T, год	T proof, год (клапан)	PFDavg
4	1	5,31E-04

Пример. Расчет вероятности отказа на запрос

СПИК СЗМА

Время работы, год	**sensor** PFDavg Tproof	**PLC** PFDavg Tproof	**final elem** PFDavg Tproof	**PFDavg контура**	**УПБ**
4	5.53E-04 **–**	0.076E-04 **–**	12.8E-04 **–**	**1.84E-03**	**2**
4	3.33E-04 **1 год**	0.076E-04 **–**	12.8E-04 **–**	**1.62E-03**	**2**
4	3.00E-04 **6 мес**	0.076E-04 **–**	12.8E-04 **–**	**1.59E-03**	**2**
4	3.33E-04 **1 год**	0.076E-04 **–**	5.31E-04 **1 год**	**8.72E-03**	**3**
4	3.00E-04 **6 мес**	0.076E-04 **–**	5.31E-04 **1 год**	**8.39E-03**	**3**
3	3.33E-04 **1 год**	0.057E-04 **–**	9.46E-04 **–**	**1.28E-03**	**2**
3	3.00E-04 **6 мес**	0.057E-04 **–**	9.46E-04 **–**	**1.25E-03**	**2**
2	3.33E-04 **1 год**	0.038E-04 **–**	6.20E-04 **–**	**9.57E-04**	**3**
1	3.00E-04 **6 мес**	0.019E-04 **–**	3.05E-04 **–**	**5.67E-04**	**3**

Для случая подсистемы исполнительных элементов 1oo1

4	2.65E-04 1год	7.60E-05 **–**	3.22E-03 1 год	**3.56E-03**	**2**
4	2.43E-04 6 мес	7.60E-05 **–**	2.51E-03 6 мес	**2.83E-03**	**2**

Выводы

СПИК СЗМА

1 Подтверждение соответствия проектируемой системы ПАЗ требованиям функциональной безопасности является обязательным требованием ФНиП «ОПВБ для взрывопожароопасных, нефтехимических и нефтеперерабатывающих производств»

2 В задание на проектирование (в приложение к договору) должно быть включено требование о выполнении проектной оценки функциональной безопасности системы ПАЗ

3 В техническом задании на создание системы ПАЗ или в задании на проектирование КИПиА, выдаваемом технологическим отделом, должен быть приведен перечень контуров ПАЗ с назначенными УПБ

4 При проектировании системы ПАЗ определение структуры и выбор компонентов контуров ПАЗ должны производиться с учетом показателей отказоустойчивости и надежности, установленных в ГОСТ Р МЭК 61511

5 В техническом задании (или технических требованиях) на систему ПАЗ должны быть включены требования по времени восстановления и интервалам времени между проверками технических средств системы ПАЗ

СПАСИБО
за внимание!

Вопросы?

mailto:info@szma.com

дополнительная информация

www.szma.com/sil.shtml