СПИК СЗМА

Специализированная инжиниринговая компания

Севзапмонтажавтоматика

г. Санкт-Петербург

СПИК СЗМА

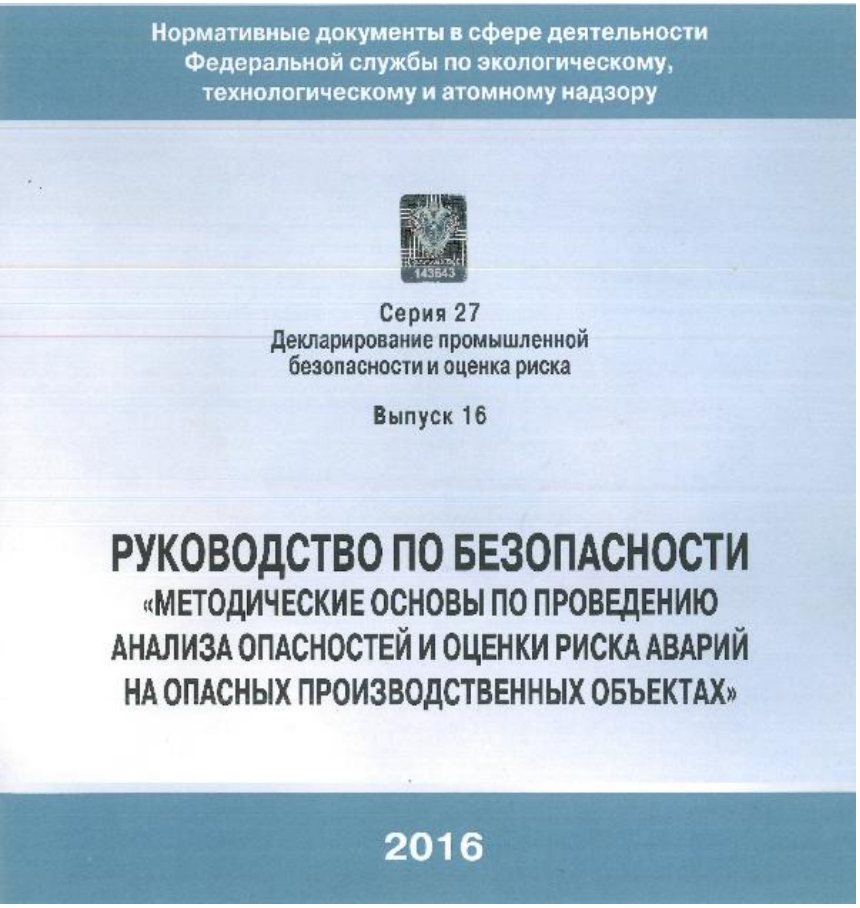
ISO 9001:2008

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

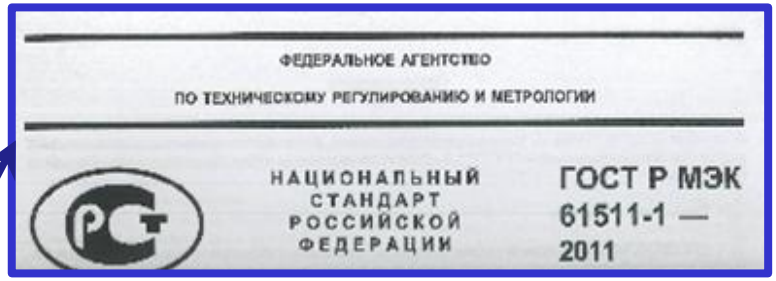
Программно-методическое обеспечение проектной оценки показателей функциональной безопасности систем противоаварийной защиты опасных производственных объектов

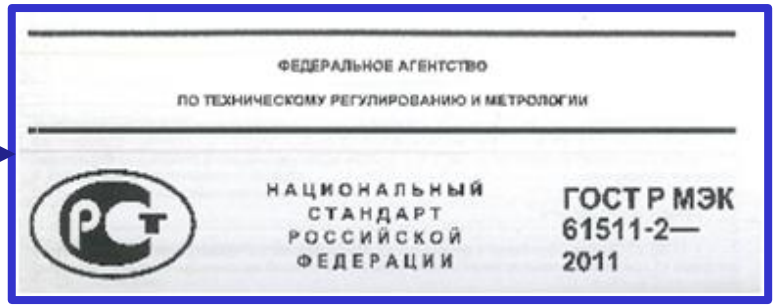
XX ВСЕРОССИЙСКАЯ
НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ И БЕЗОПАСНОСТИ»
«Риск-ориентированные технологии обеспечения безопасности на потенциально опасных объектах в современных условиях»
Санкт-Петербург,
05 апреля 2017 года

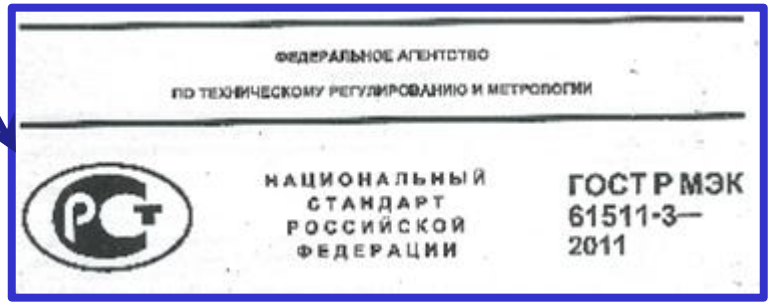
Российское Научное Общество Анализа Риска



46. При анализе опасностей, связанных с отказами технических устройств, систем обнаружения утечек, автоматизированных систем управления технологическим процессом (АСУТП), систем противоаварийной защиты (ПАЗ) рекомендуется анализировать технический риск, показатели которого определяются соответствующими **методами теории надежности**.







В основе стандартов серии 61511 лежат две фундаментальные концепции:

- концепция ЖЦ безопасности;
- концепция УПБ.

УПБ	Минимально допустимое число отказов		
	SSF (ДБО)<60%	SSF (ДБО)960%	SSF (ДБО)>60%
1	1	0	0
2	2	1	0
3	3	2	1
4	Специальные требования		

1

Минимально необходимые требования к архитектуре канала

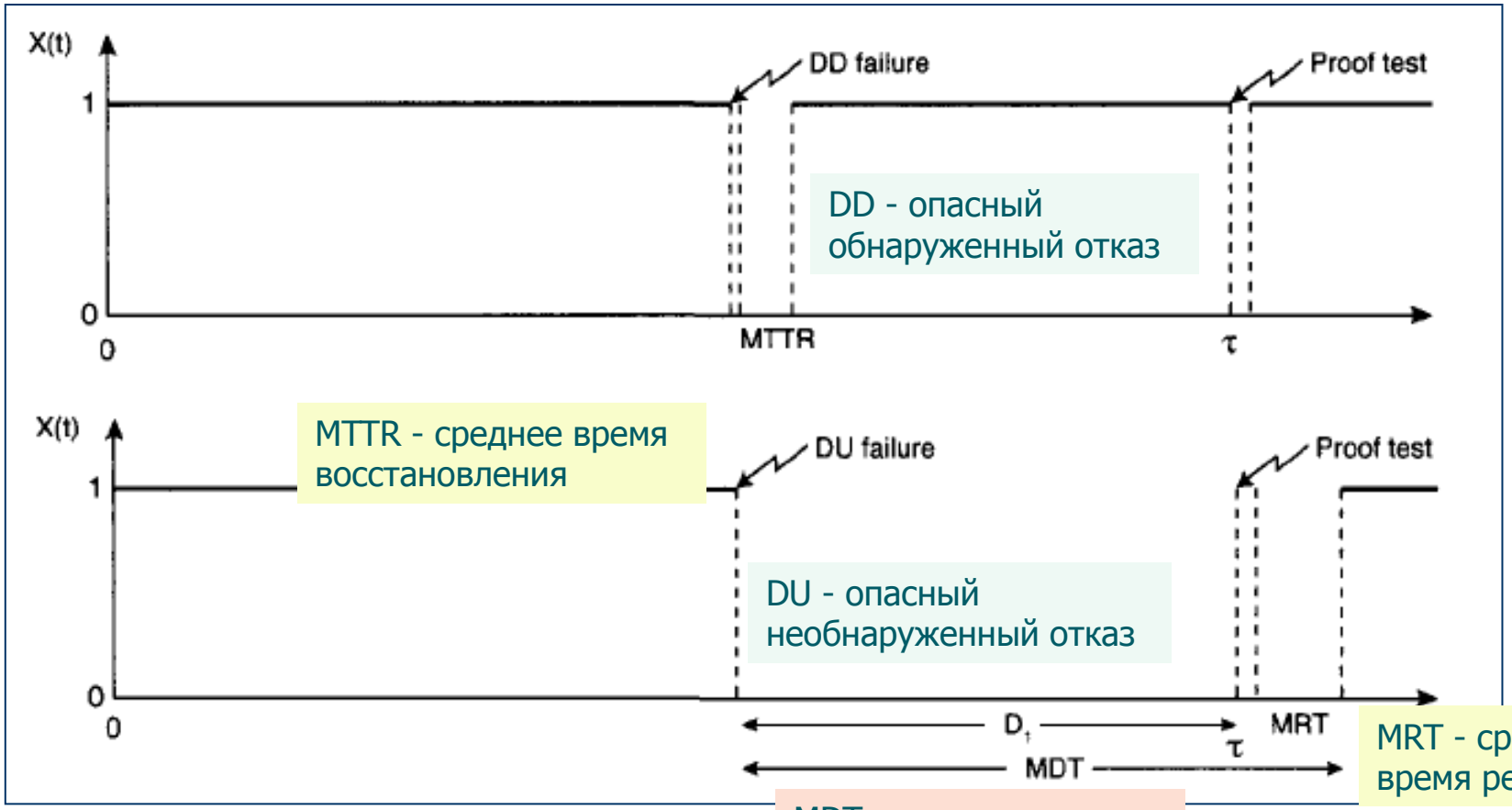
2

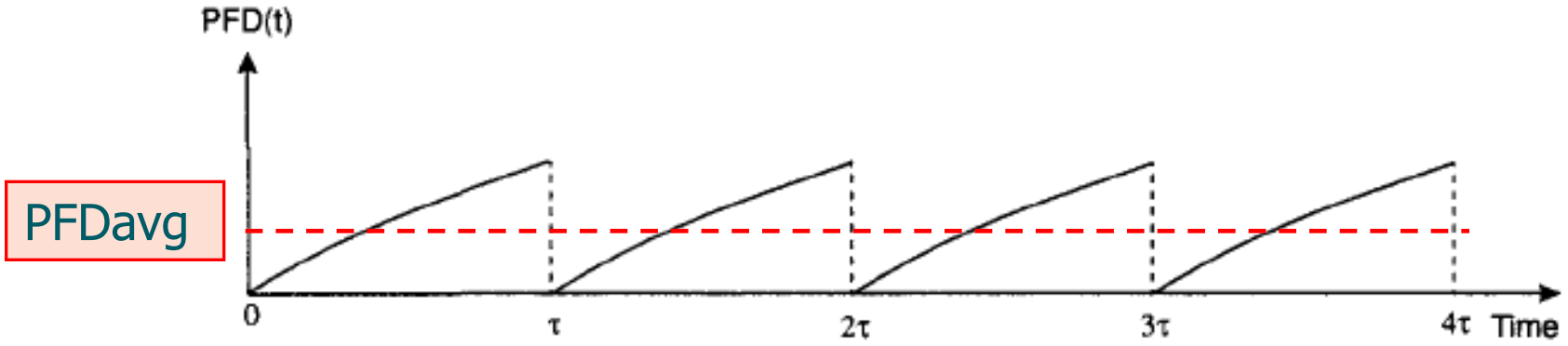
Уровень безопасности (SIL)	Режим с низким уровнем требований по требованию функции безопасности (средняя вероятность отказа в выполнении заданной функции безопасности по требованию)	Режим с высоким уровнем требований по требованию функции безопасности (вероятность опасного отказа в течении одного часа в режиме непрерывной работы)
4	$\geq 10^{-5}$ PFD $< 10^{-4}$	$\geq 10^{-9}$ PFH $< 10^{-8}$
3	$\geq 10^{-4}$ PFD $< 10^{-3}$	$\geq 10^{-8}$ PFH $< 10^{-7}$
2	$\geq 10^{-3}$ PFD $< 10^{-2}$	$\geq 10^{-7}$ PFH $< 10^{-6}$
1	$\geq 10^{-2}$ PFD $< 10^{-1}$	$\geq 10^{-6}$ PFH $< 10^{-5}$

3

Подбор компонентов, расчет PFD и уточнение архитектуры элементов канала

Расчет *PFD* основан на учете двух типов неготовности канала:
1 - неизвестная, когда простой 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.





Неготовность на межпроверочном интервале есть отношение среднего времени простоя **E(D₁)** к величине межпроверочного интервала τ, то есть

$$\mathrm{PFD} = \frac{E(D_1)}{\tau}$$

Среднее время простоя на межпроверочном интервале вычисляется как

$$E(D_1) = \int_0^{\tau} F(t)\,dt$$

где, ***F(t)*** – вероятность отказа канала.

Тогда

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{1}{\tau}\int_0^{\tau} \mathrm{PFD}(t)\,dt = \frac{1}{\tau}\int_0^{\tau} F(t)\,dt = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)\,dt$$

где, ***R(t)*** – вероятность безотказной работы канала.

Алгоритмическая основа Методики - приближенные формулы стандарта IEC 61508-6 для расчета PFD_{avg} простых типовых архитектур.

Основные допущения моделей расчета PFD:

- все каналы имею постоянную интенсивность отказов (λ_I=const);
- все резервированные каналы имеют одинаковые интенсивности отказов и процент диагностического покрытия DC...

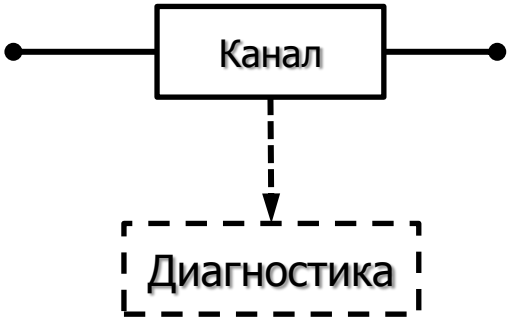
Основная идея IEC 61508-6 состоит в расчете PFD_{avg} канала, представленного как один элемент.

Расчет базируется на использовании средней групповой частоты опасных отказов λ_{DG} и эквивалентном групповом времени простоя t_{GE}.

$$PFD^{(G)}_{avg} = F(\lambda_{D,G}, t_{GE}, T1, MTTR, MTR)$$

Базовыми архитектурами для структурного анализа функциональной безопасности реальных ПАЗ выбраны :

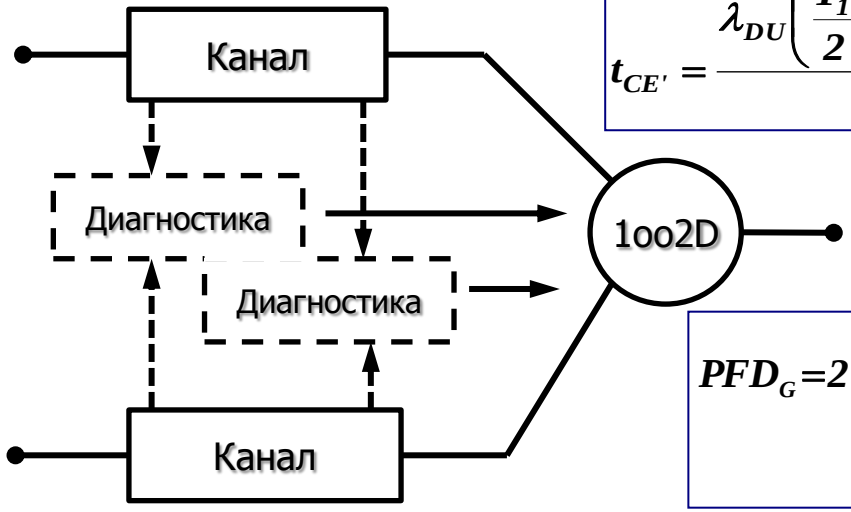
архитектура 1oo1



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

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

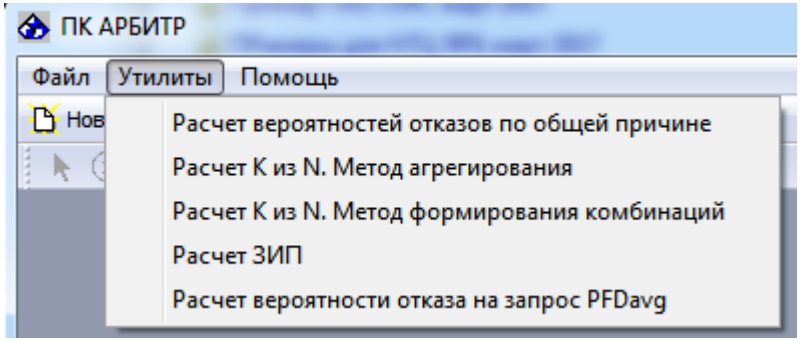
архитектура 1oo2D

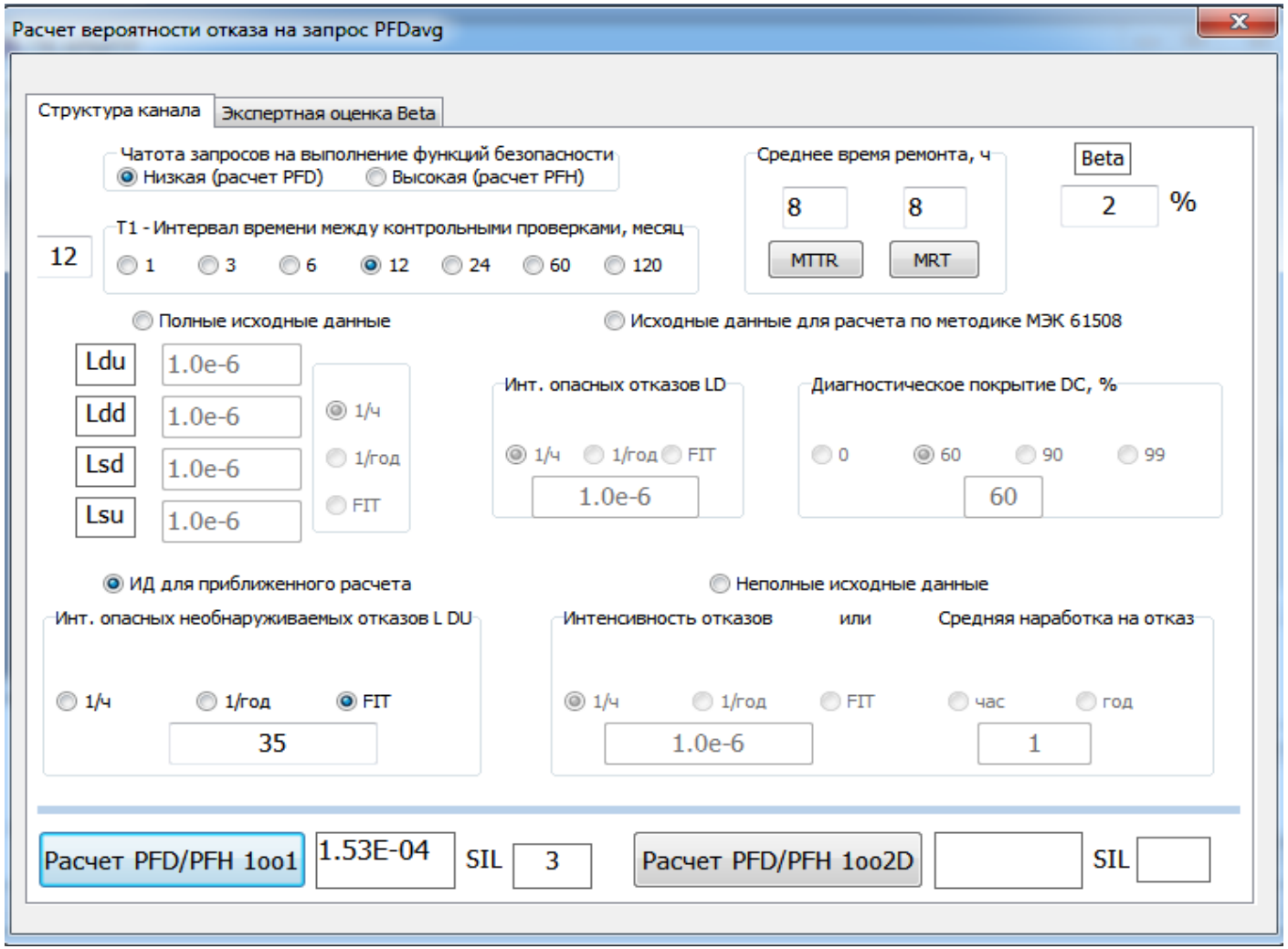


$$t_{CE'} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})}, \quad t_{GE'} = \frac{T_1}{3} + MRT.$$

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta)\lambda_{DD} + \lambda_{SD})t_{CE'}t_{GE'} + \\ + 2(1-K)\lambda_{DD}t_{CE'} + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right).$$

Для подготовки исходных данных разработана утилита
« Расчет вероятности отказа на запрос *PFDavg*»





МЕТОДИКА ОЦЕНКИ ВЕРОЯТНОСТЕЙ ОТКАЗА АППАРАТНЫХ СРЕДСТВ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ (ПАЗ)

1. Основные термины и определения

2. Общие положения

2.1 Методы и подходы

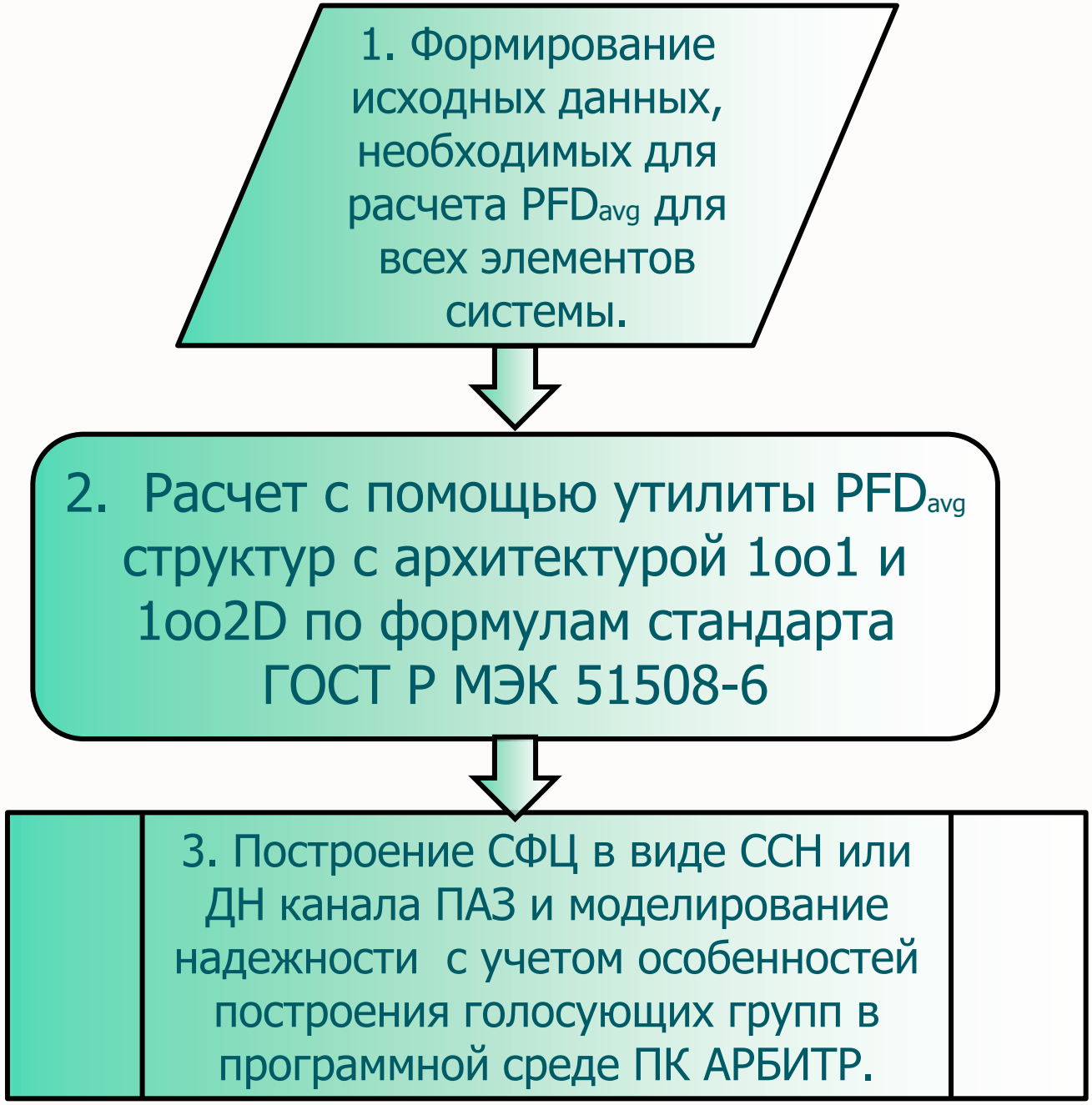
2.2 Предположения

2.3 Содержание методики

2.3.1 Формирование исходных данных

2.3.2. Расчет с помощью утилиты вероятностей отказа на запрос

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


1. Формирование исходных данных, необходимых для расчета PFDavg для всех элементов системы.
2. Расчет с помощью утилиты PFDavg структур с архитектурой 1oo1 и 1oo2D по формулам стандарта ГОСТ Р МЭК 51508-6
3. Построение СФЦ в виде ССН или ДН канала ПАЗ и моделирование надежности с учетом особенностей построения голосующих групп в программной среде ПК АРБИТР.

По физическому смыслу PFD есть средняя неготовность системы на интервале между контрольными проверками.
Так как состояние системы безопасности полностью определяется состоянием ее элементов, тогда

$$PFDsys = P\{PFD_1,...,PFD_i,....,PFD_n\},$$
$$PFHsys = P\{PFH_1,...,PFH_i,....,PFH_n\},$$

где $PFDsys, PFHsys$ - системные показатели функциональной безопасности;

$\boldsymbol{PFD_i, PFH_i}$ - показатели функциональной безопасности i-го компонента;

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

Пример 1 (МЭК 61508-6)

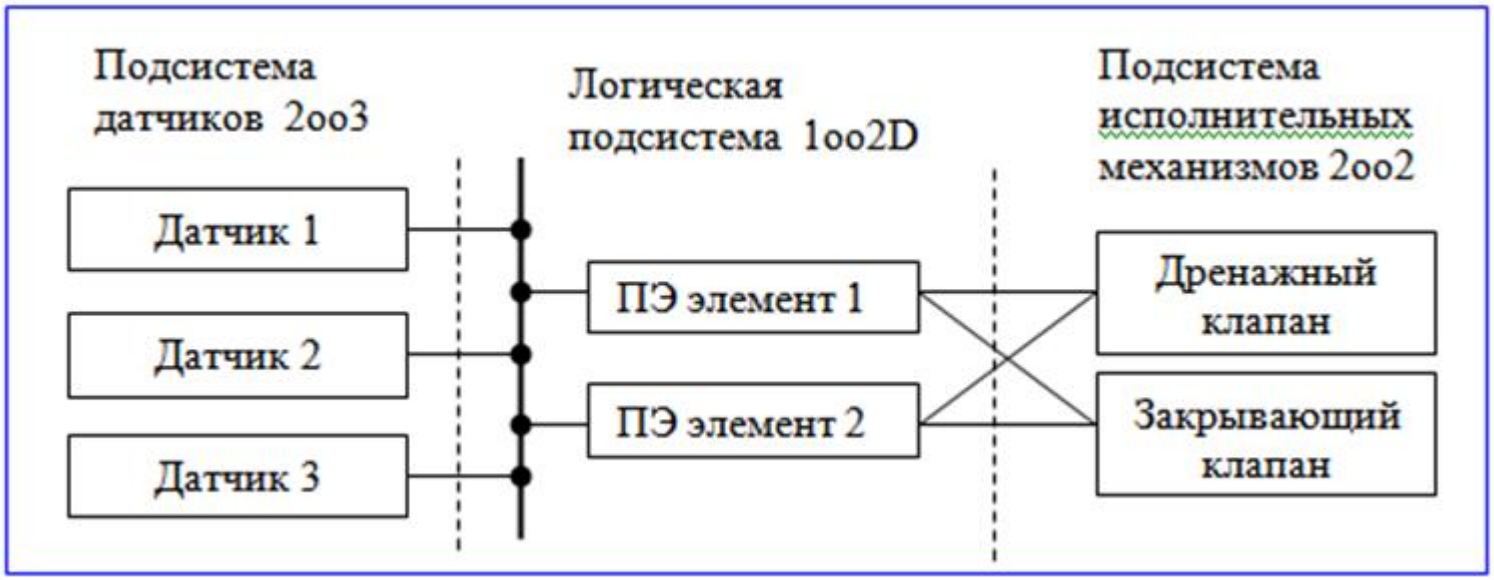


Рисунок В.14 – Архитектура системы рассматриваемого примера для режима низкой интенсивности запросов

1. Формирование исходных данных, необходимых для расчета PFD для всех элементов системы.

I. ИД для всего канала:

1. Частота запросов на выполнение ФБ – низкая;
2. Интервал времени между контрольными проверками T_1=12 мес.
3. Среднее время восстановления и средняя продолжительность ремонта MTTR= MRT=8ч.

II. ИД по компонентам канала

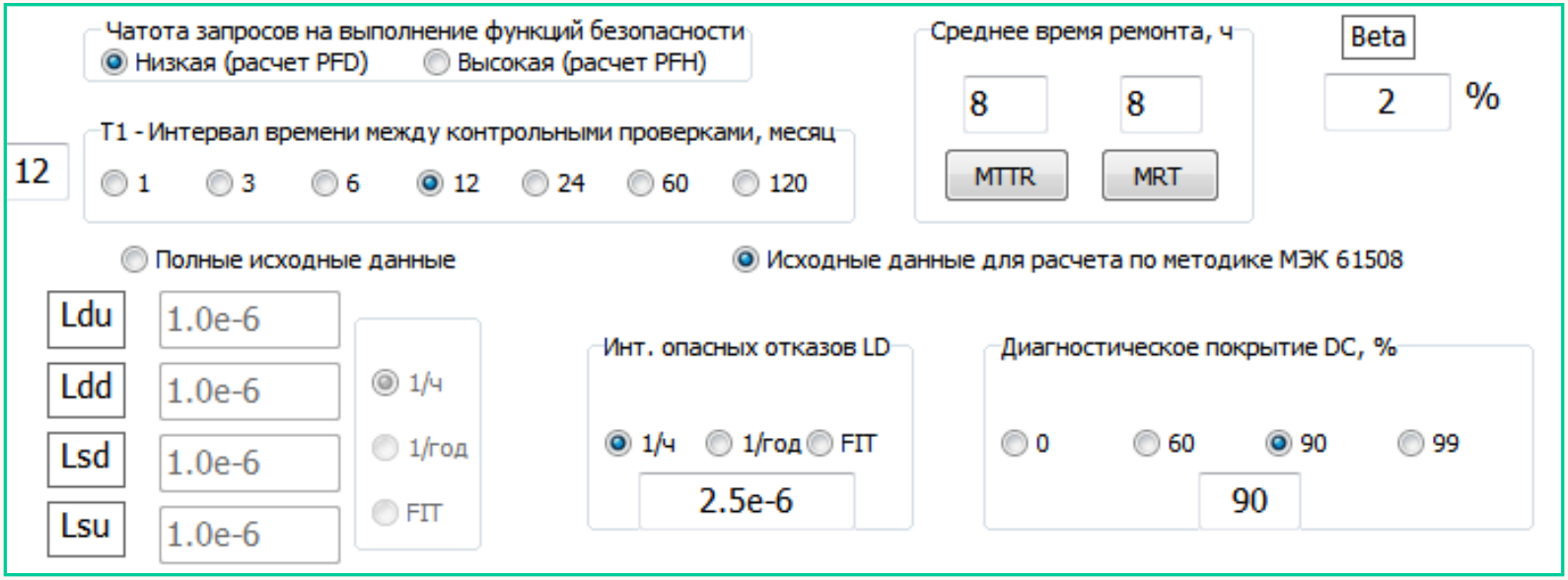
Наименование элементов	λ_D, 1\ч	DC,%	β,%	β_D,%	T1, мес	MTR, ч
Датчики	2.5E-6	90	20	10	12	8
ПЭ логические элементы	5.0-6	99	2	1	12	8
Дренажный клапан	2.5E-6	60	-	-	12	8
Закрывающий клапан	5.0-6	60	-	-	12	8

III. ИД по архитектуре элементов канала

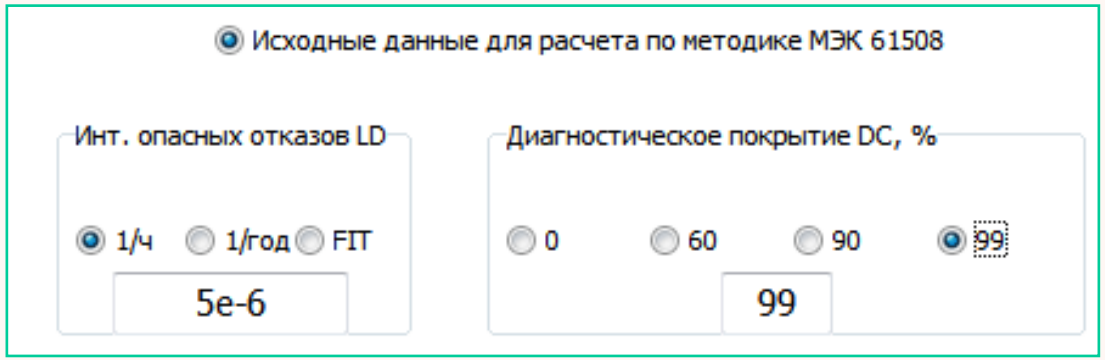
Наименование элементов	Архитектура
Датчики	2oo3
ПЭ логические элементы	1oo2D
Дренажный клапан	2oo2
Закрывающий клапан	

2. Расчет с помощью утилиты PFD структур с архитектурой 1oo1 и 1oo2D по формулам стандарта ГОСТ Р МЭК 51508-6

Пример ввода ИД для датчика



Пример ввода ИД для элемента логической подсистемы



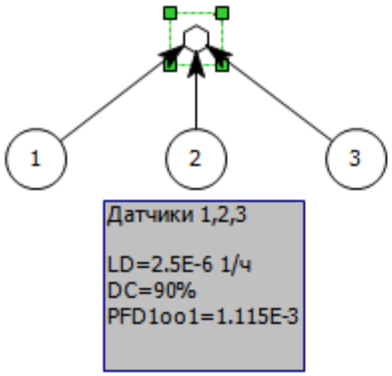
Результаты расчета

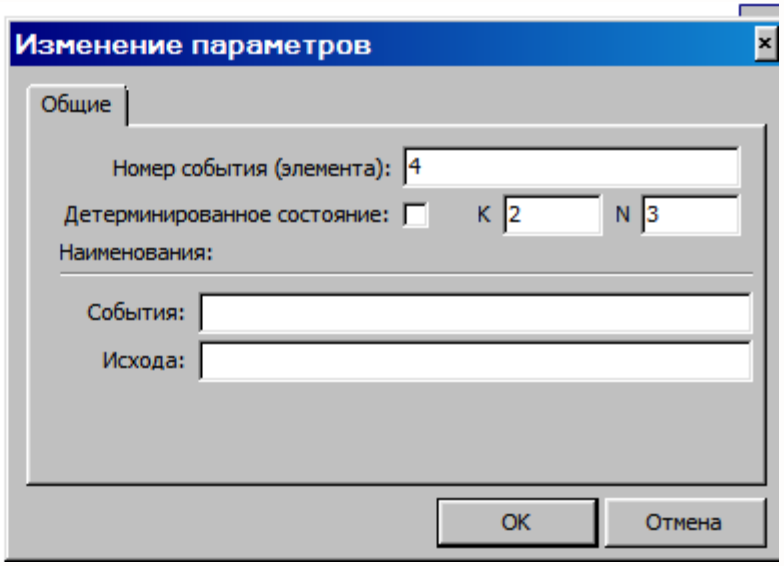
Наименование элементов	Архитектура	PFD
Датчики	1oo1	1.115·E-03
ПЭ логические элементы	1oo2D	1.042·E-05
Дренажный клапан	1oo1	4.40·E-03
Закрывающий клапан	1oo1	8.80·E-03

3. Построение СФЦ в виде ССН или ДН канала ПАЗ и моделирование надежности с учетом особенностей построения голосующих групп в программной среде ПК АРБИТР.

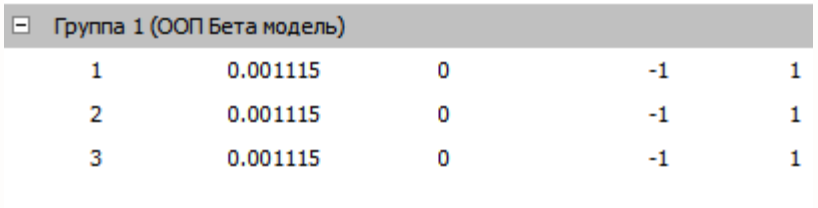
Моделирование надежности подсистемы датчиков

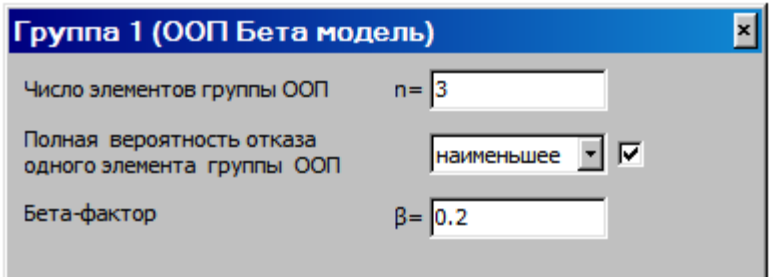
а) ДН с архитектурой 2оо3



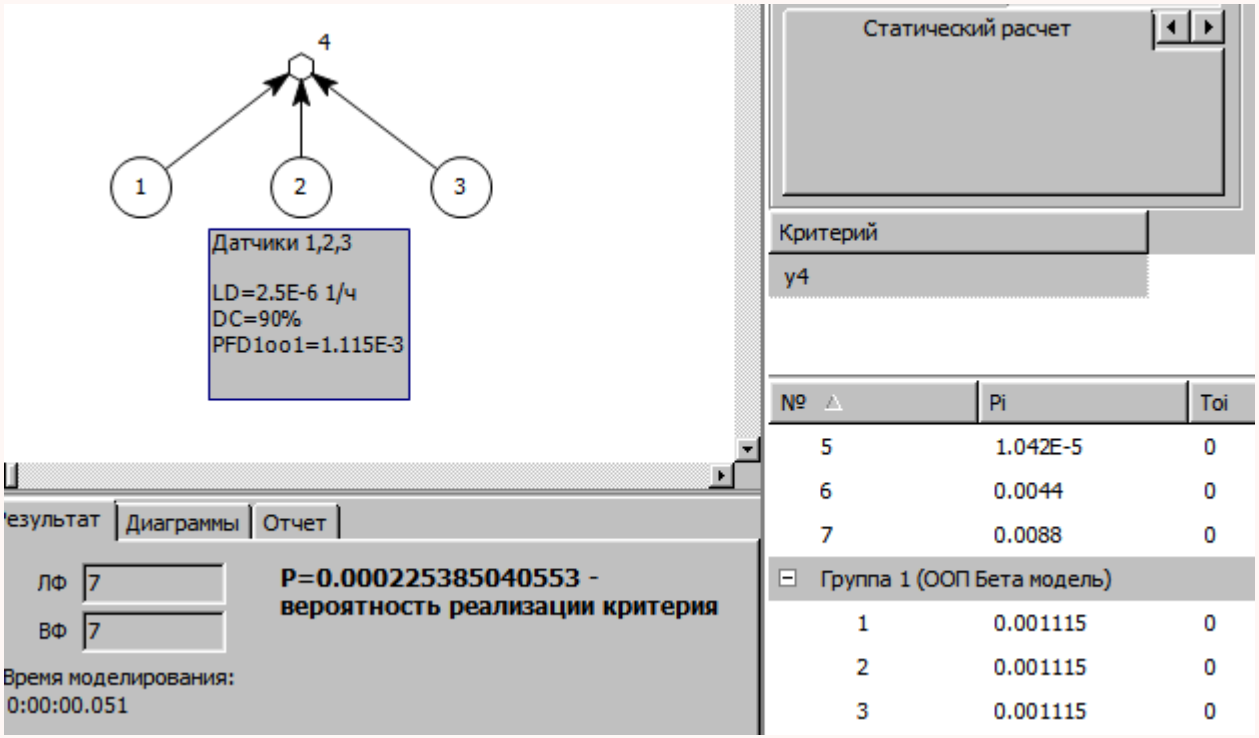


б) группа ООП



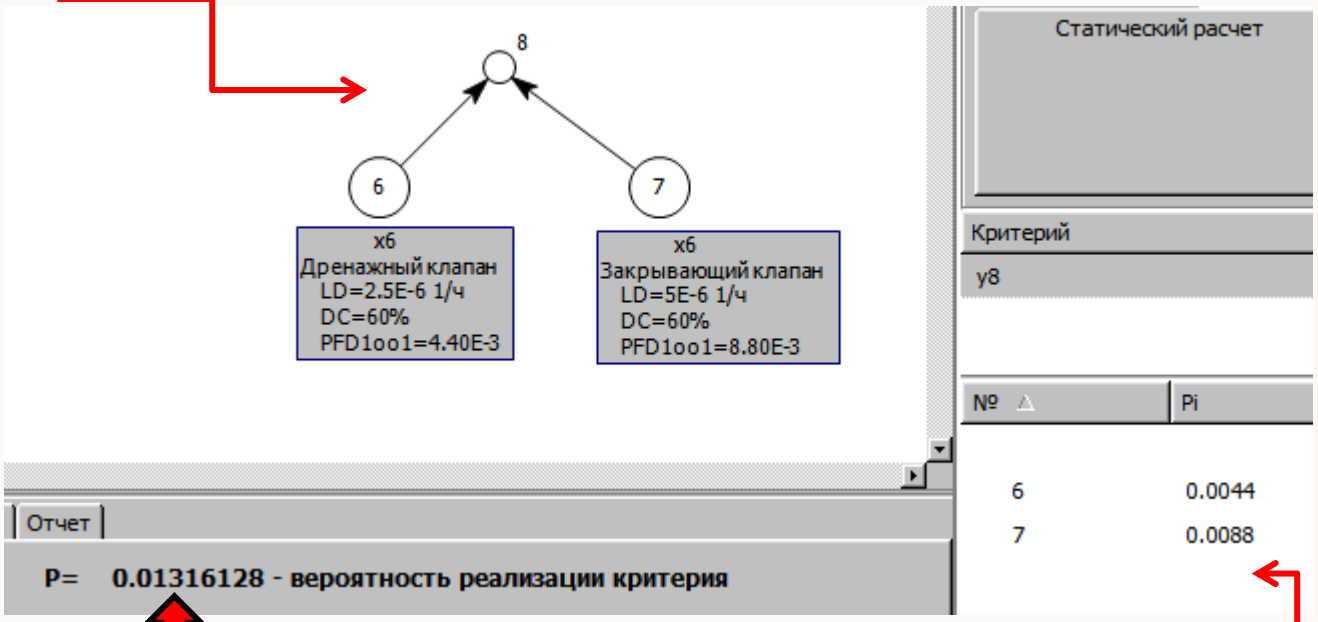


Результаты моделирования надежности подсистемы датчиков



Моделирование надежности подсистемы исполнительных механизмов

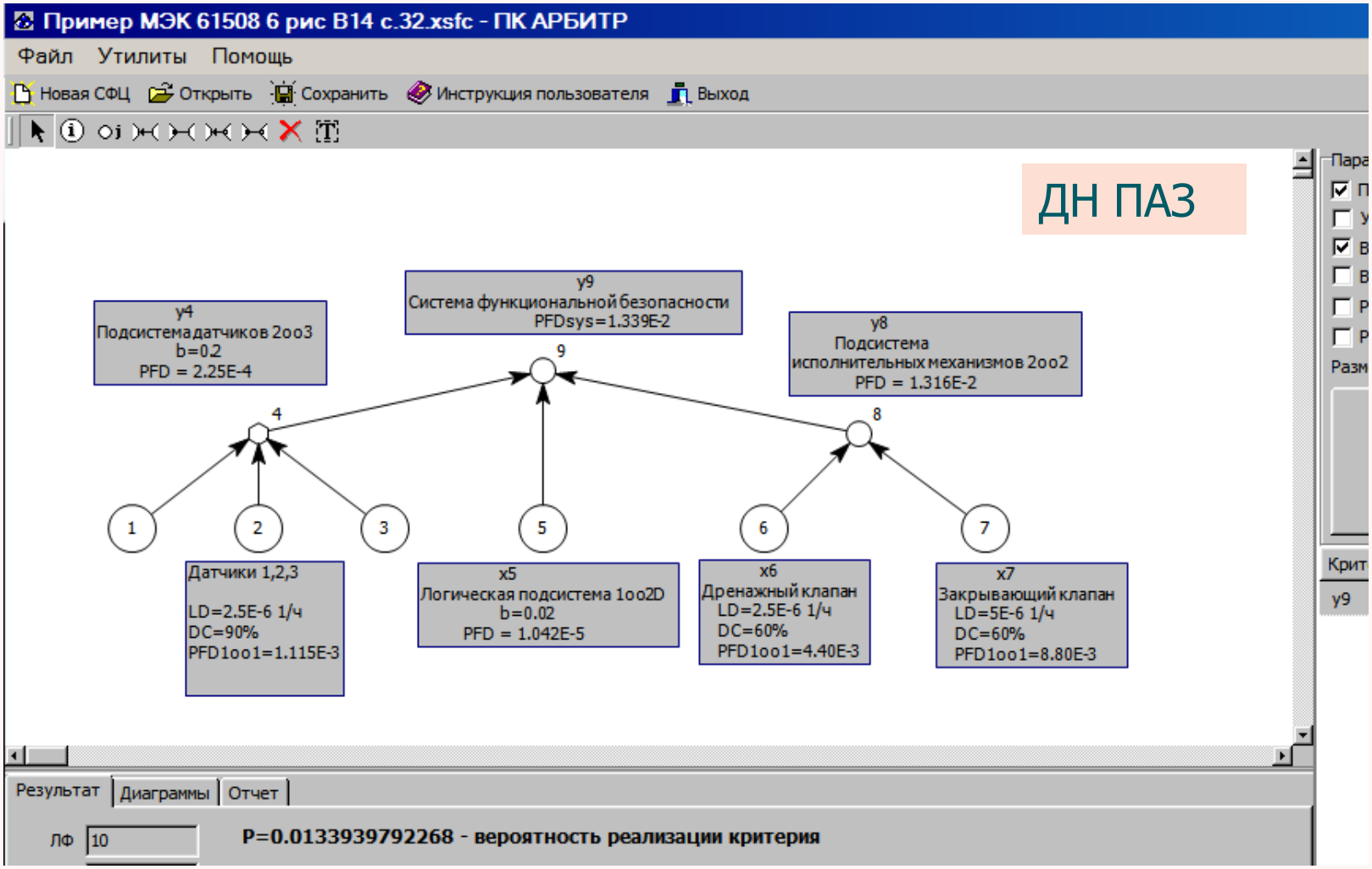
ДН исполнительных механизмов



Результаты моделирования

Исходные данные

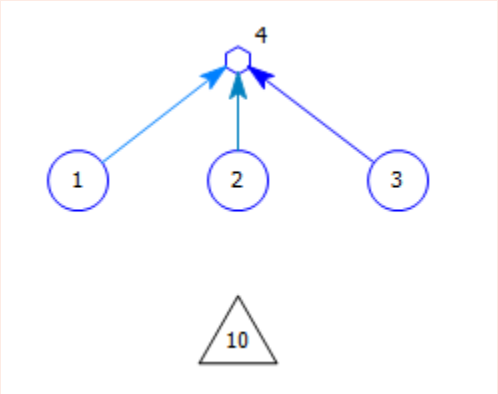
Моделирование надежности ПАЗ



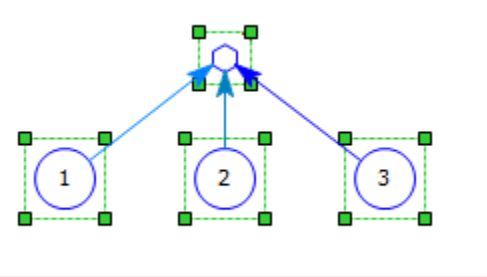
Результаты моделирования: PFDsys=1.34E-04; **SIL1**

Формирование редуцированной СФЦ

1. Создание эквивалентированной вершины №10 для подсистемы датчиков

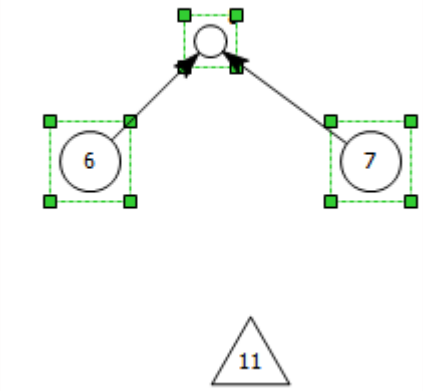


2. Копирование архитектуры подсистемы датчиков и перенос ее в вершину №10

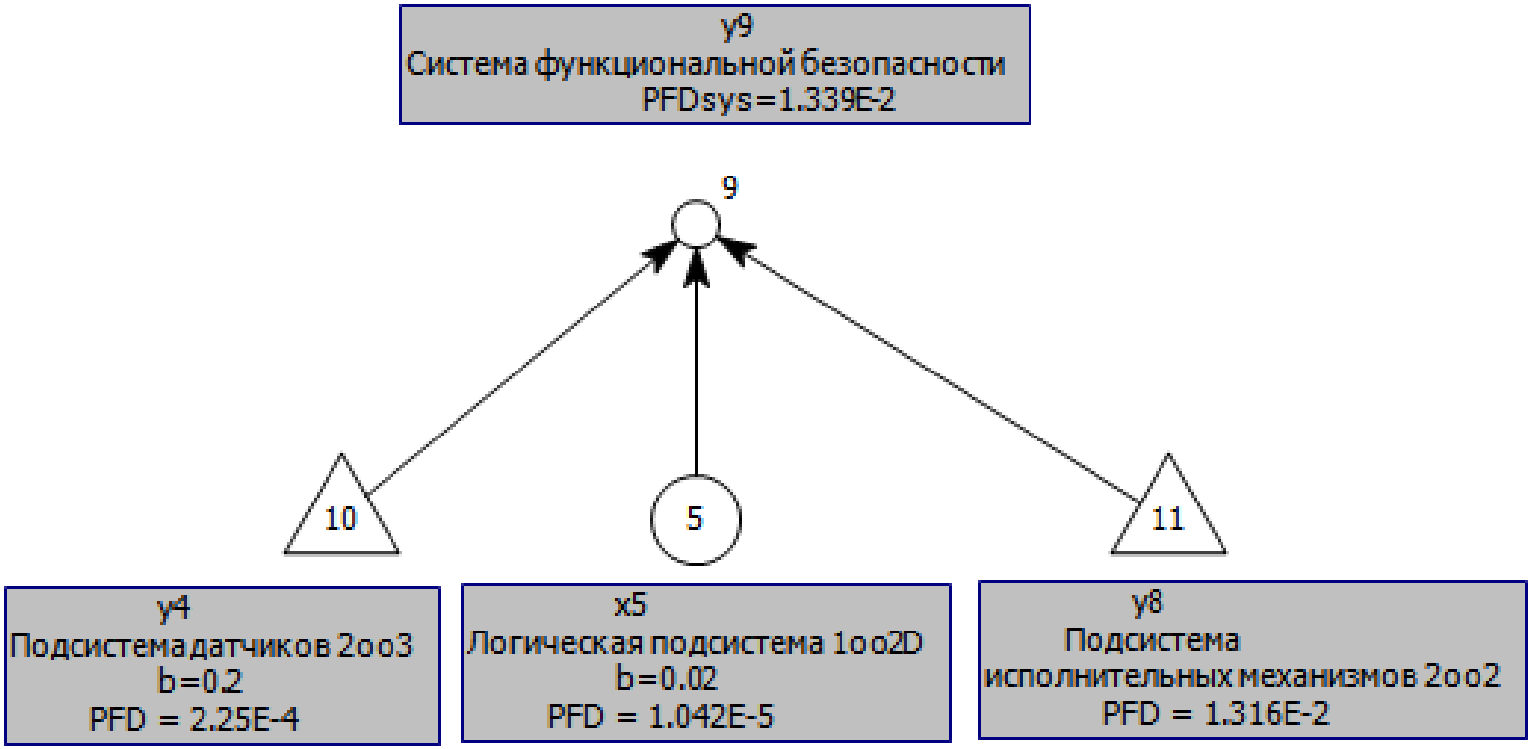


3. Создание эквивалентированной вершины №11 для подсистемы исполнительных механизмов

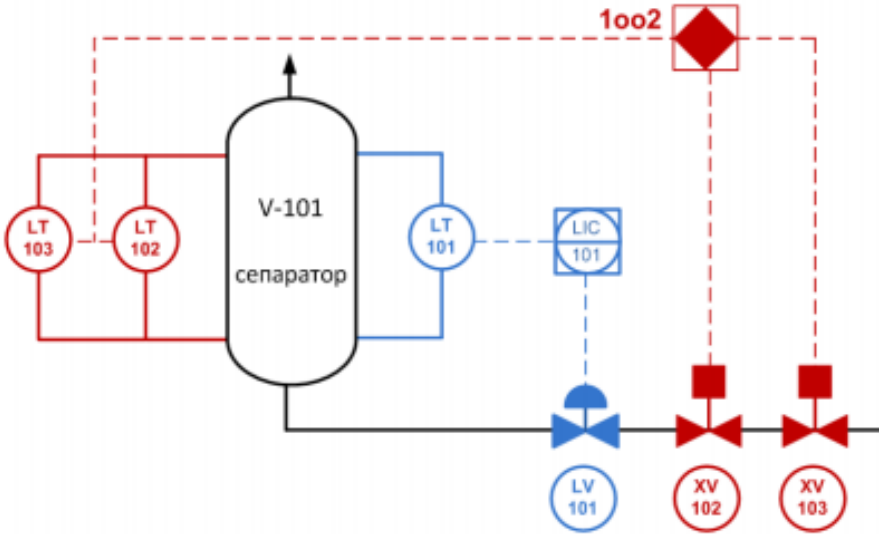
4. Копирование архитектуры подсистемы исполнительных механизмов и перенос ее в вершину №11



Формирование редуцированной СФЦ



Пример 2 Подтверждение УПБ контура ПАЗ



Исходные данные для расчета PFD подсистемы подключения датчиков

Обозначение	№ СФЦ ДН	Элемент	Производитель	Ls (FIT)	Ldd (FIT)	Ldu (FIT)	MTBF (г)	**PFD расч**
D1, D2	101, 106	Датчик уровня	VEGA	7	0	35	358	1.53E-04
Б1, Б2	102, 107	Барьер	MTL	116	210	17		7.45E-05
AI-1, AI-2	103, 108	Модуль AI	Siemens				26.5	4.72E-03
IM1.1-IM2.2	104,105, 109,110	Интерф.модуль	Siemens				106	1.18E-03

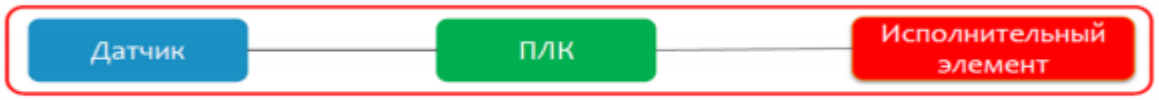
Исходные данные для расчета PFD подсистемы ПЛК

Обозначение	№ СФЦ ДН	Элемент	Производитель	Ls (FIT)	Ldd (FIT)	Ldu (FIT)	MTBF (г)	**PFD расч**
CPU1,CPU2	111, 112	ПЛК	Siemens				30	4.167E-03

Исходные данные для расчета PFD подсистемы подключения ИМ

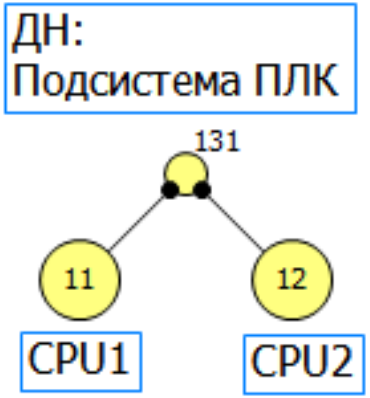
Обозначение	№ СФЦ ДН	Элемент	Производитель	Ls (FIT)	Ldd (FIT)	Ldu (FIT)	MTBF (г)	PFD	PFD расч
D01, D02	115, 120	Модуль DO	Siemens					2.0·E-9 (1/ч)	1.53E-04
P1, P2	116, 121	Реле	GM				113		1.11E-03
ИМ1, ИМ2	117, 122	Привод	Auma			647			4.72E-03
IM3.1-IM4.2	113,114, 118,119	Интерф.модуль	Siemens				106		1.18E-03

ГОСТ Р МЭК 61511-2



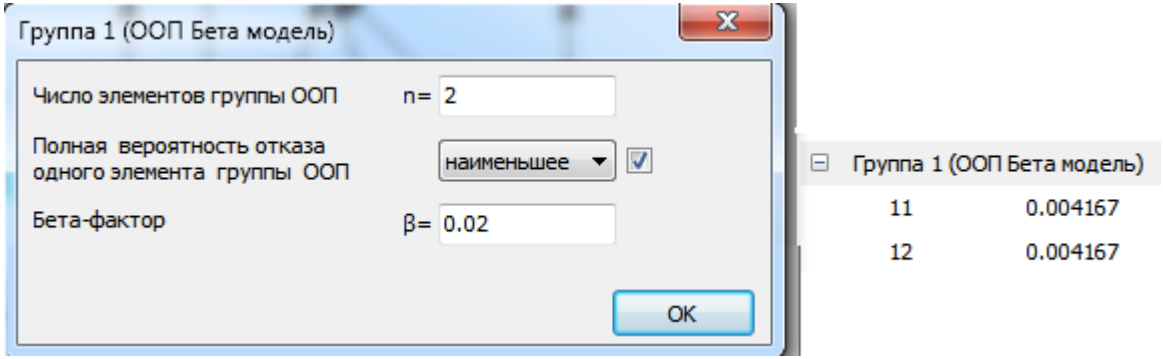
$$PFD_{контур} = PFD_{датчик} + PFD_{ПЛК} + PFD_{Испол\ Элемент}$$

Подсистема ПЛК (архитектура 1oo2)



1. Составление СФЦ в виде ДН

2. Формирование группы ООП и ввод параметров бета-модели

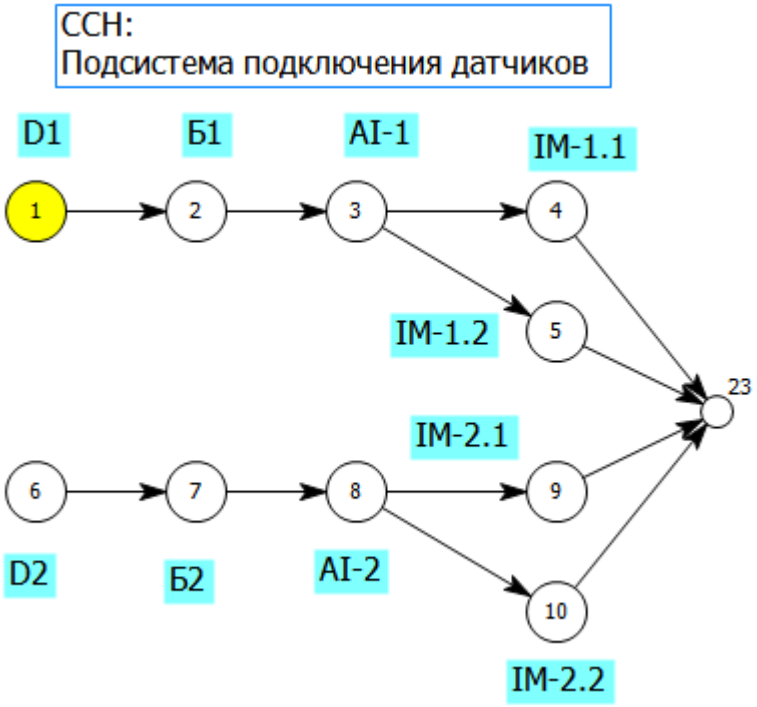


Группа 1 (ООП Бета модель)	
11	0.004167
12	0.004167

3. Расчет по критерию y132 : ⇒ PFDплк = 1,0·E-04 (1/год)

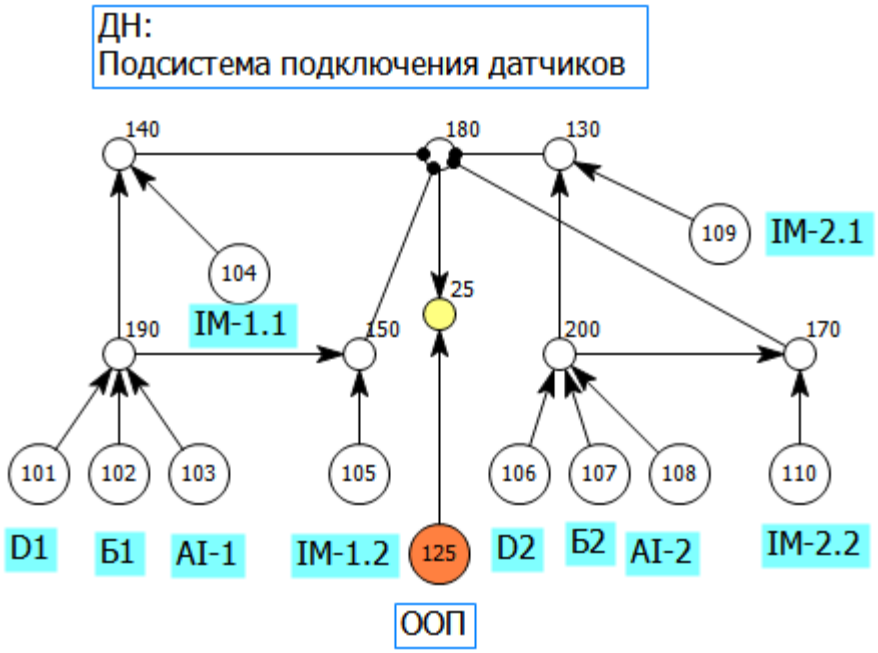
Подсистема подключения датчиков (канальная архитектура 1oo2)

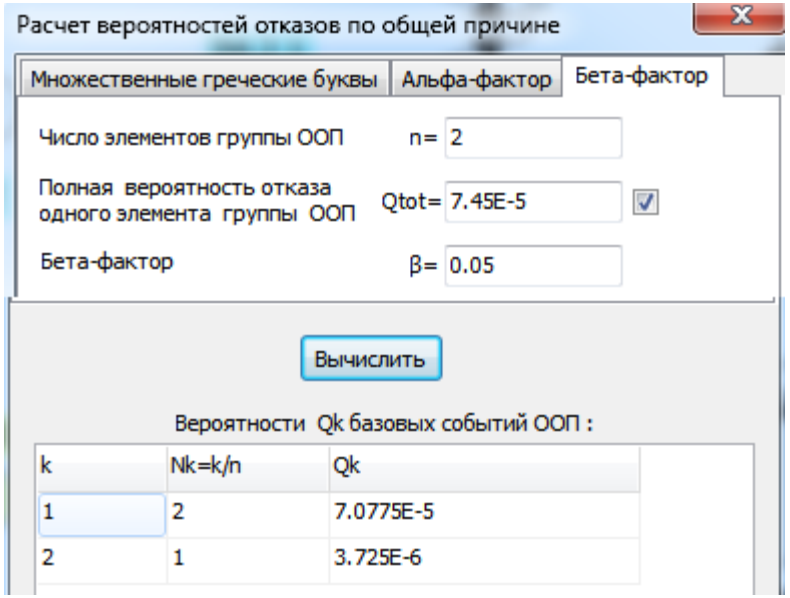
1. Составление СФЦ в виде ССН



2. Решение по инверсному критерию y”23 и формирование минимальных сечений отказов

3. Составление СФЦ в виде ДН с учетом модели ООП



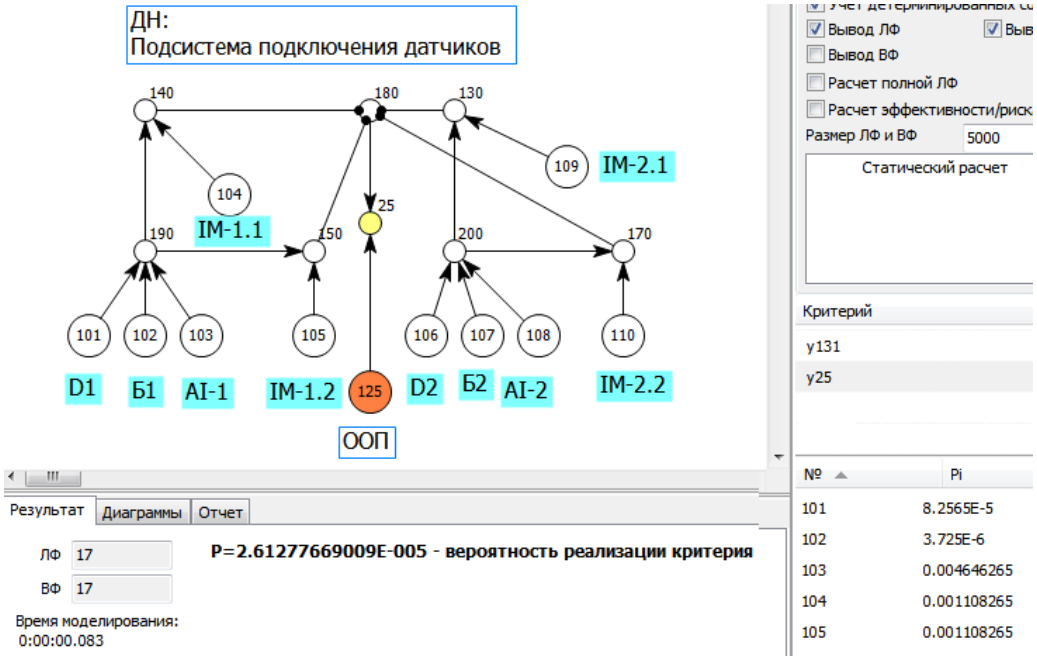


4. Расчет параметров группы ООП.
Базовым элементов является элемент с минимальным значением PFD

5. Пересчет значений PFD элементов с учетом модели CCF

Обозначение	№ вершин	Элемент	PFD расч 1 год	CCF=b*minPFD	dCCF	**PFD-dCCF**
D1, D2	101, 106	Датчик уровня	1.53E-04			8.26E-05
Б1, Б2	102, 107	Барьер	7.45E-05	3.73E-06	7.0735E-05	3.73E-06
AI-1, AI-2	103, 108	Модуль AI	4.72E-03			4.65E-03
IM1.1-IM1.4	104,105, 109,110	Интерф.модуль	1.18E-03			1.11E-03

6. Ввод значений PFD элементов и расчет по критерию y25:



PFDпд=2.61E-05

Подсистема подключения исполнительных механизмов (канальная архитектура 1oo2)

1. Составление СФЦ в виде ССН

2. Решение ССН по инверсному критерию и формирование минимальных сечений отказов

3. Составление СФЦ в виде ДН с учетом модели ООП

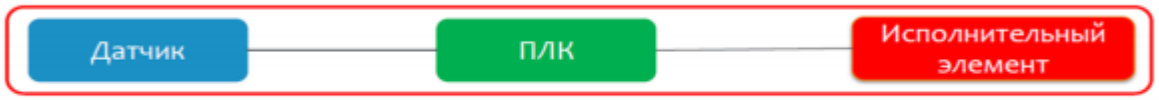
4. Расчет параметров группы ООП

5. Пересчет значений PFD элементов с учетом модели CCF

6. Ввод значений PFD элементов и расчет по системному критерию.

PFDпд=1.63E-05

ГОСТ Р МЭК 61511-2



$$PFD_{контур} = PFD_{датчик} + PFD_{ПЛК} + PFD_{Испол\ Элемент}$$

PFD $_{контур}$ =2.61E-05 + 1.00E-04 + 1.63E-05 = 1.26E-04

УПБ = 3

Доклад закончен, спасибо за внимание!

Можаева Ирина Александровна

Струков Александр Владимирович

info@szma.com