# СПИК СЗМА

## Специализированная инжиниринговая компания

## Севзапмонтажавтоматика

г. Санкт-Петербург

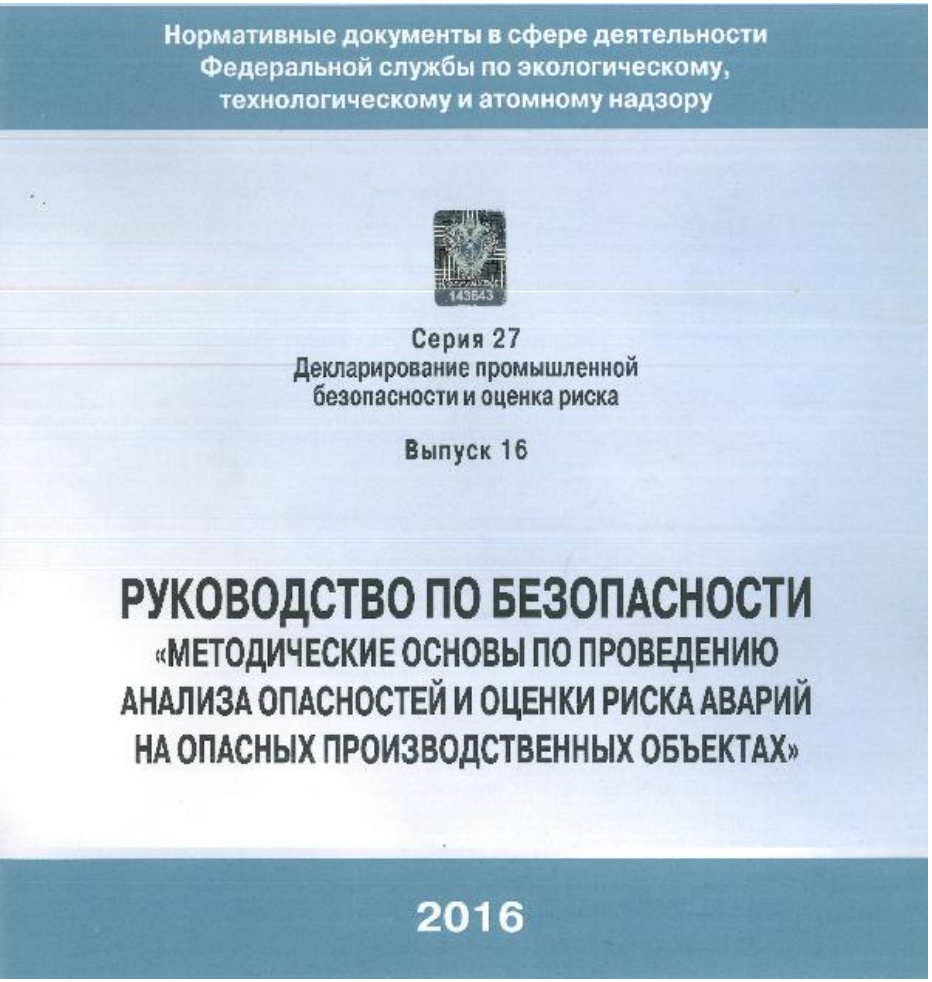
СПИК СЗМА

ISO 9001:2008

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

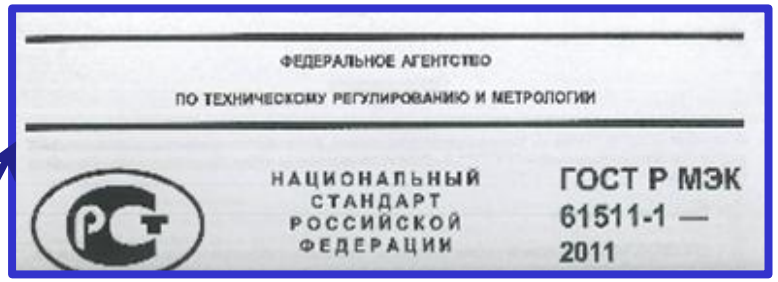
# ПРИМЕНЕНИЕ ПК АРБИТР ДЛЯ ПРОЕКТНОЙ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ

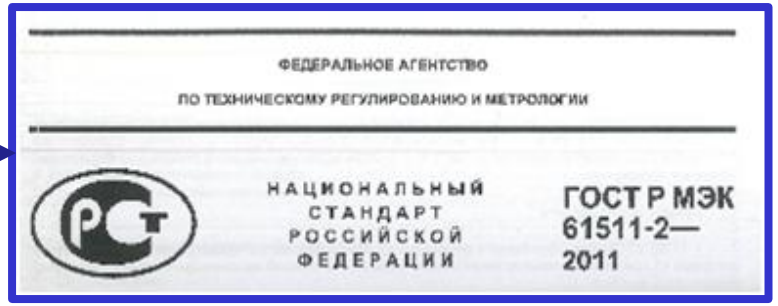
**Международная научно-практическая конференция**
**ИКМ МТМТС-2017**
**Санкт-Петербург,**
**28 июня 2017 года**

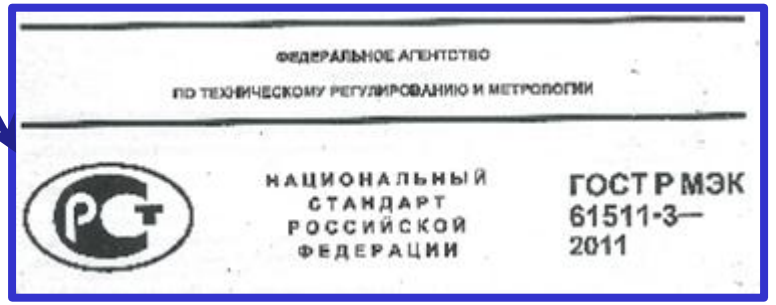



46. При анализе опасностей, связанных с отказами технических устройств, систем обнаружения утечек, автоматизированных систем управления технологическим процессом (АСУТП), систем противоаварийной защиты (ПАЗ) рекомендуется анализировать технический риск, показатели которого определяются соответствующими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

Методы расчета надежности технических систем рекомендуется сочетать с методами **моделирования аварий** и количественной оценки риска аварий.

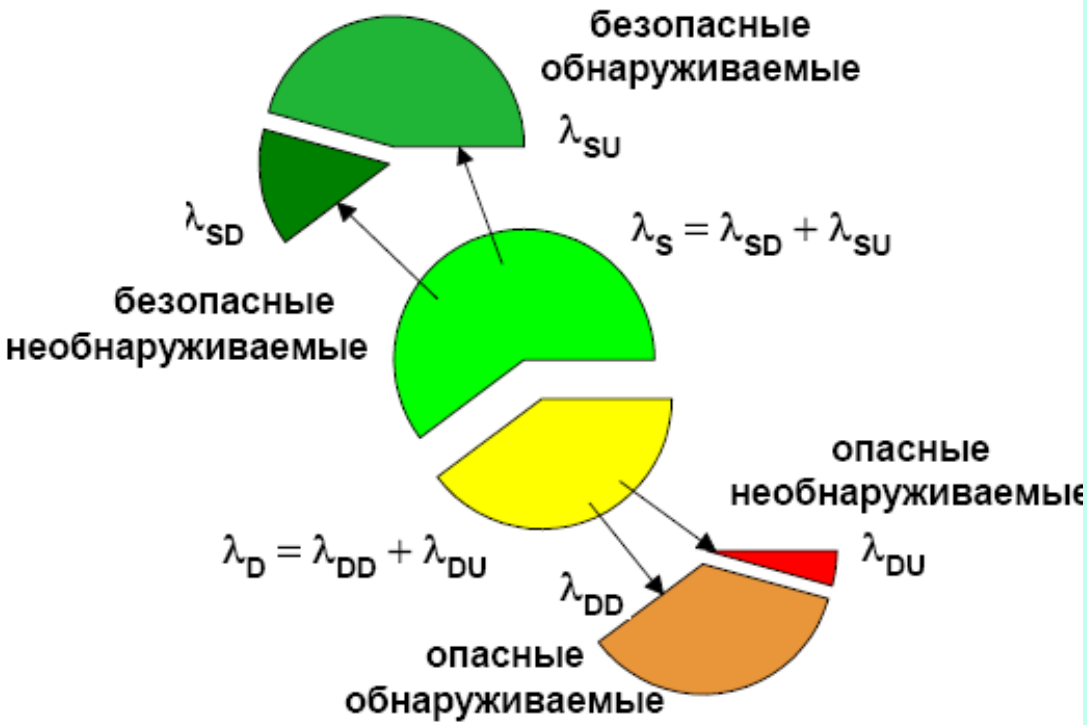




В основе стандартов серии 61511 лежат две фундаментальные концепции:

- концепция ЖЦ безопасности;
- концепция УПБ.




| Обозначение | Тип отказа |
|---|---|
| $\lambda_S$ | безопасный отказ |
| $\lambda_{SD}$ | безопасный обнаруживаемый отказ |
| $\lambda_{SU}$ | безопасный необнаруживаемый отказ |
| $\lambda_D$ | опасный отказ |
| $\lambda_{DD}$ | опасный обнаруживаемый отказ |
| $\lambda_{DU}$ | опасный необнаруживаемый отказ |

(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.

Обнаруженный отказ:

- Установленный с помощью диагностических проверок, контрольных проверок, вмешательства оператора..

| 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

## Необходимые требования к архитектуре канала

2

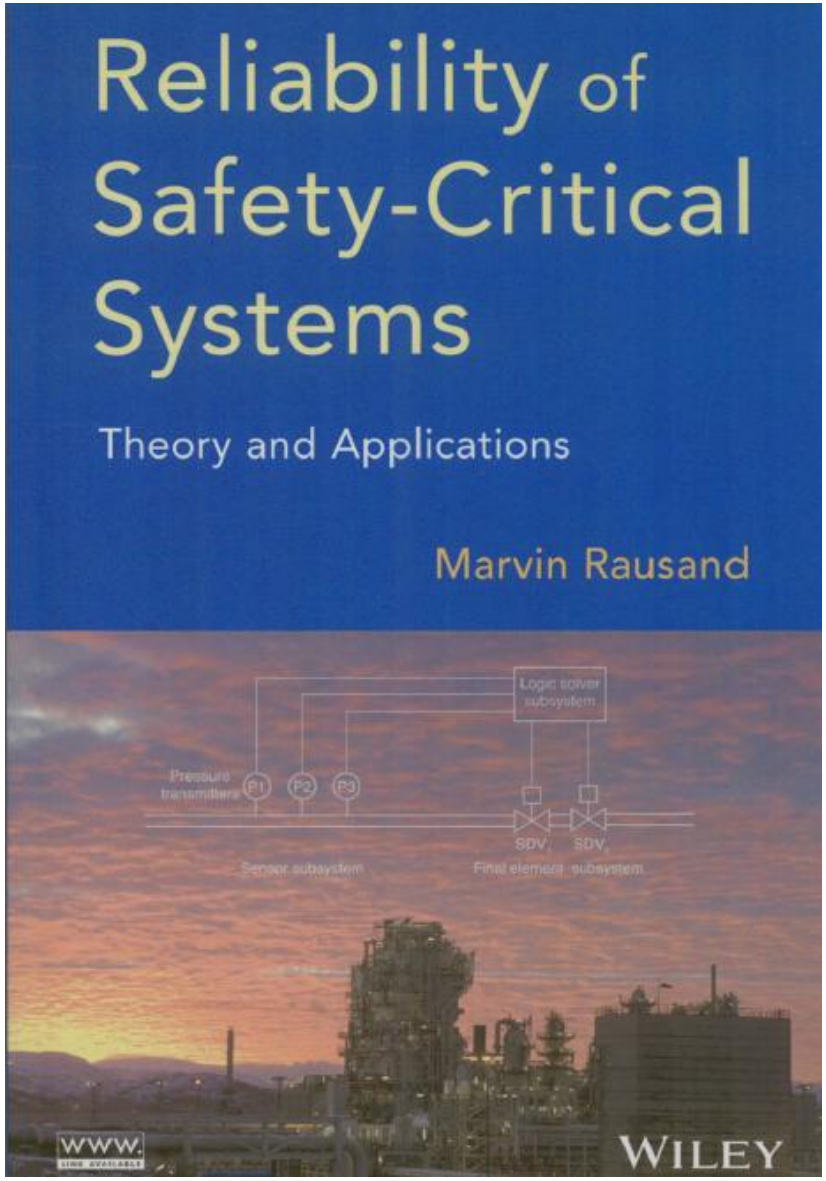
| **Уровень безопасности (SIL)** | **Режим с низким уровнем требований по требованию функции безопасности** (средняя вероятность отказа в выполнении заданной функции безопасности по требованию) | **Режим с высоким уровнем требований по требованию функции безопасности** (вероятность опасного отказа в течение 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

| Архитек-тура | Описание |
|---|---|
| 1oo1 | Архитектура состоит из одного канала. Любой возникающий в ней опас-ный отказ приводит к отказу функции безопасности при обращении к ней. |
| 1oo2 | Архитектура состоит из двух дублирующих друг друга каналов. Каждый канал в состоянии самостоятельно и независимо обеспечить выполнение функции безопасности. Поэтому опасный отказ должен произойти в обоих каналах, чтобы привести к отказу фунции безопасности при обращении к ней (логика построения И). |
| 2oo2 | Архитектура состоит из двух параллельных каналов. Каждый канал должен самостоятельно обеспечить выполнение функции безопасности для того чтобы она могла быть выполнена при обращении к ней (логика построения ИЛИ). |
| 2oo3 | Архитектура состоит из трёх дублирующих друг друга каналов, связанных с устройством мажоритарного выбора. Состояние на выходе архитектуры остается неизменным, если даже один канал выдает результат отличный от обоих других. |

Архитектура – конкретная конфигурация элементов аппаратного и программного обеспечения системы




Стандарт IEC61508-6 приводит приближенные формулы для расчета $PFD_{avg}$ для простых архитектур с числом каналов не более 3. Формулы приведены без каких-либо выводов и объяснений.

Основная идея IEC61508-6 состоит в расчете PFDavg канала, представленного как один элемент.

Расчет базируется на использовании средней групповой частоте опасных отказов $\lambda_{DG}$ и эквивалентном групповом времени простоя $t_{GE}$. Тогда

$$PFD_{avg}^{(G)} = \lambda_{D,G} t_{GE}$$

## Основные допущения моделей расчета PFD:

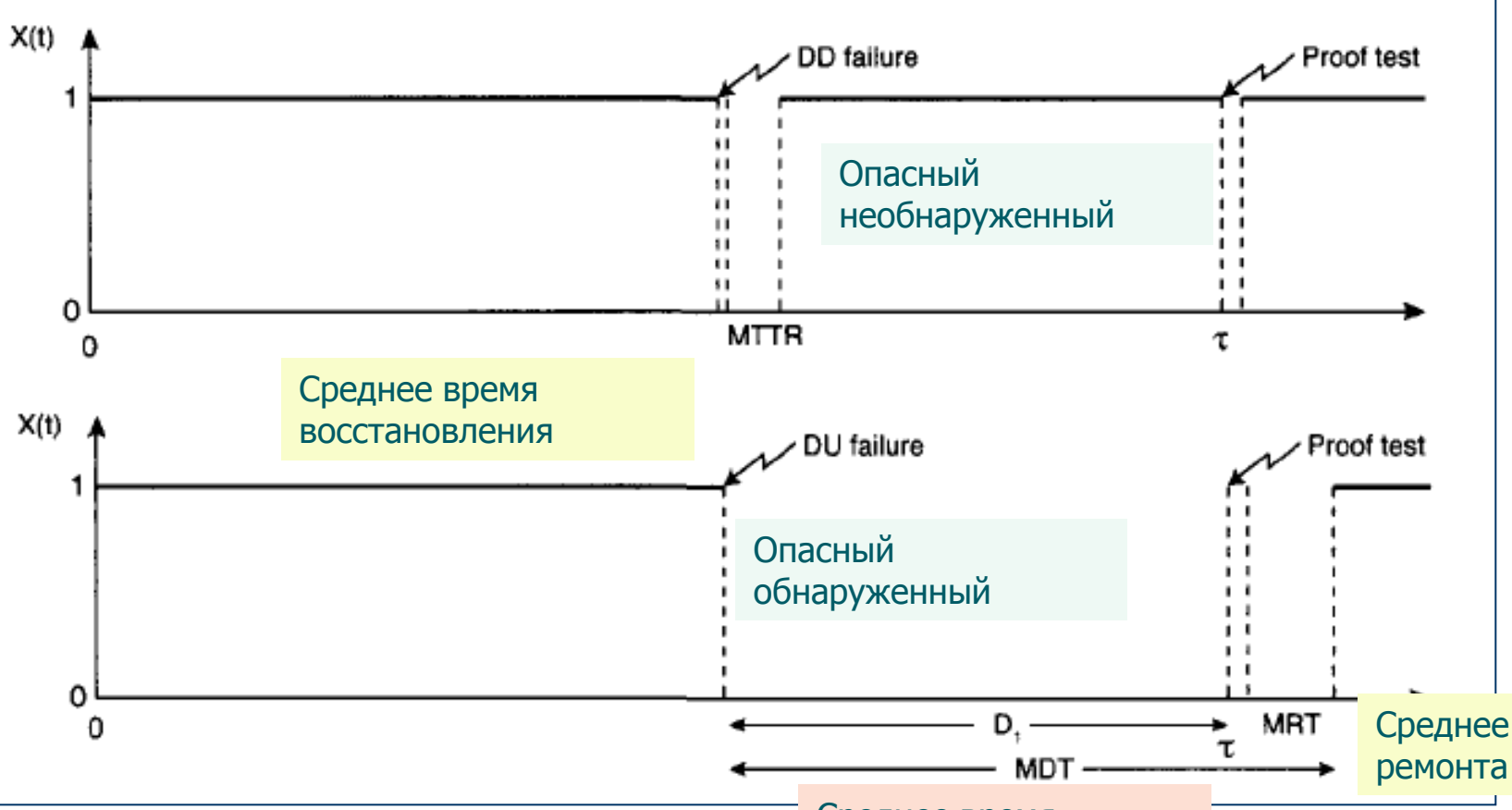
- все каналы имею постоянную интенсивность отказов ($\lambda_I = const$);

- Все каналы периодически контролируются. Если во время проверки обнаружен отказ – осуществляется ремонт длительностью

MRT <<0.1·T1 ($\tau$);

- Если во время функционирования обнаружен опасный отказ (DU) – осуществляется восстановление длительностью MTTR;

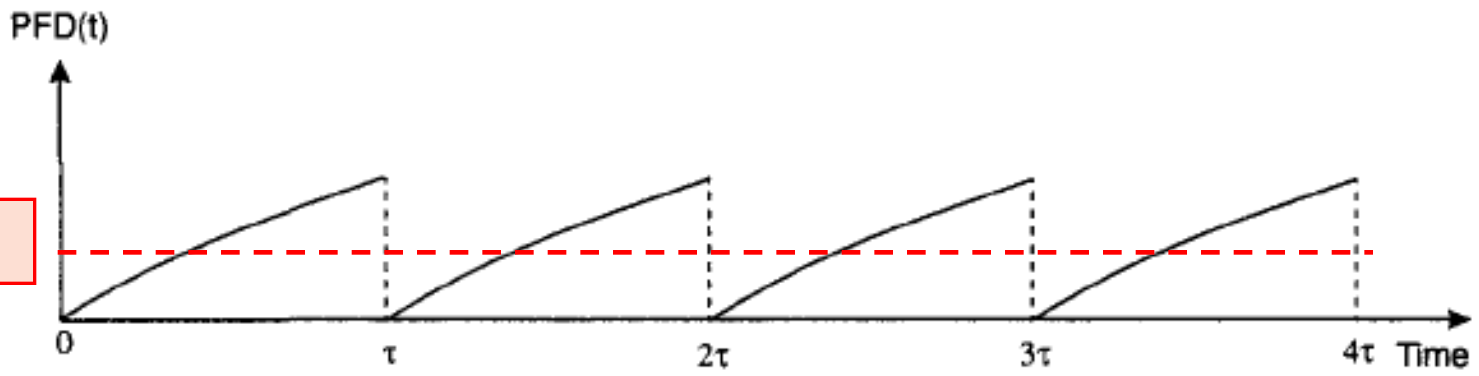
- Все резервированные каналы имеют одинаковые интенсивности отказов и процент диагностического покрытия DC;
- Ожидаемое время между запросами на функционирование ПАЗ по крайней мере в 10 раз превышает T1;
- Учет ООП проводится с использованием бета-модели отдельно для DD и DU отказов.




2 типа неготовности:

*неизвестная*, когда простой вызван DD (опасными необнаруженными) или DU (опасными обнаруженными) отказами;

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




PFDavg – средняя неготовность ПАЗ на межпроверочном интервале.

Так как неготовность на межпроверочном интервале есть отношение среднего времени простоя $D_1$ к величине межпроверочного интервала, то $$PFD = \frac{E(D_1)}{\tau}$$

Среднее время простоя на межпроверочном интервале вычисляется как $$E(D_1) = \int_0^{\tau} F(t)dt$$

Тогда $$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} PFD(t)dt = \frac{1}{\tau}\int_0^{\tau} F(t)dt = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)dt$$

## Для структуры 1oo1:

$$PFD = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)dt = 1 - \frac{1}{\tau}\int_0^{\tau} e^{-\lambda_{DU}t}dt = 1 - \frac{1}{\lambda_{DU}\tau}(1 - e^{-\lambda_{DU}\tau})$$

После разложения степенной функции в ряд Тэйлора при малых значениях $\lambda_{DU}\tau$ получим: $PFD \approx \frac{\lambda_{DU}\tau}{2}$

## Для структуры 2oo1 (дублированная система):

$$R(t) = 2e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t}$$

$$PFD = 1 - \frac{1}{\tau}\int_0^{\tau} 2e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t}dt =$$

$$= 1 - \frac{2}{\lambda_{DU}\tau}(1 - e^{-\lambda_{DU}\tau}) + \frac{1}{2\lambda_{DU}\tau}(1 - e^{-2\lambda_{DU}\tau})$$

или $PFD \approx \frac{1}{3}(\lambda_{DU}\tau)^2$

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

**1. Основные термины и определения**

**2. Общие положения**

**2.1 Методы и подходы**

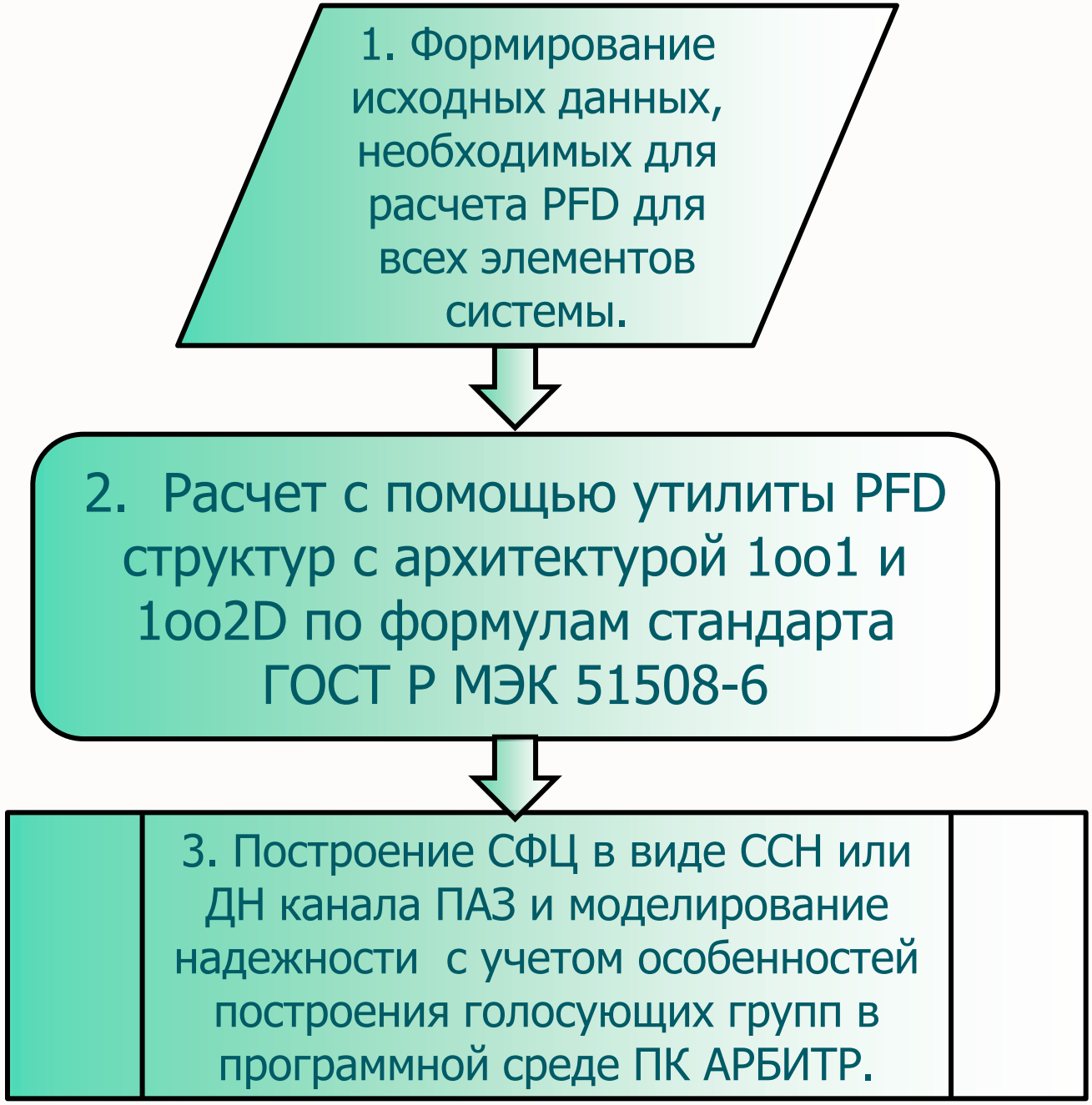
**2.2 Предположения**

**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 PFD для всех элементов системы.
2. Расчет с помощью утилиты PFD 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 , то параметрами элементов СФЦ, описывающей взаимосвязь системных показателей с показателями надежности элементов, будут показатели средней неготовности элементов. Таким образом, можно записать

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

$$PFHsys = P\{PFH_1,...,PFH_i,....,PFH_n\},$$

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

$PFD_i, PFH_i$ - показатели функциональной безопасности $i$-й компоненты;

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

# Пример 1 (МЭК 61508-6)

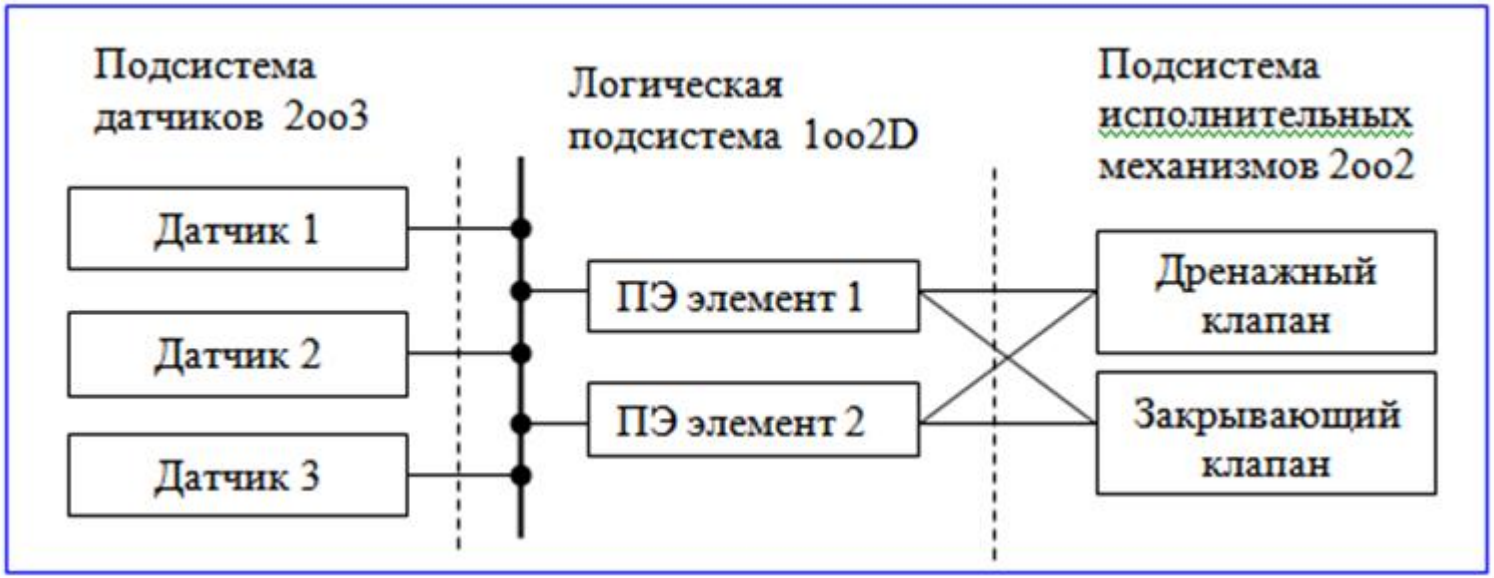



Рисунок В.14 – Архитектура системы рассматриваемого примера для режима низкой интенсивности запросов

## Исходные данные для рассматриваемого примера

| Наименование элементов | $\lambda_D$, 1/ч | DC, % | β, % | $\beta_D$, % | T1, мес | MRT, ч |
|---|---|---|---|---|---|---|
| Датчики | 2.5 E-6 | 90 | 20 | 10 | 12 | 8 |
| ПЭ логические элементы | 5.0E-6 | 99 | 2 | 1 | 12 | 8 |
| Дренажный клапан | 2.5E-6 | 60 | - | - | 12 | 8 |
| Закрывающий клапан | 5.0E-6 | 60 | - | - | 12 | 8 |

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

I. ИД для всего канала:

II. 1. Частота запросов на выполнение ФБ – низкая;

2. Интервал времени между контрольными проверками Т12 мес.

3. Среднее время восстановления и средняя продолжительность ремонта MTTR= MRT=8ч.

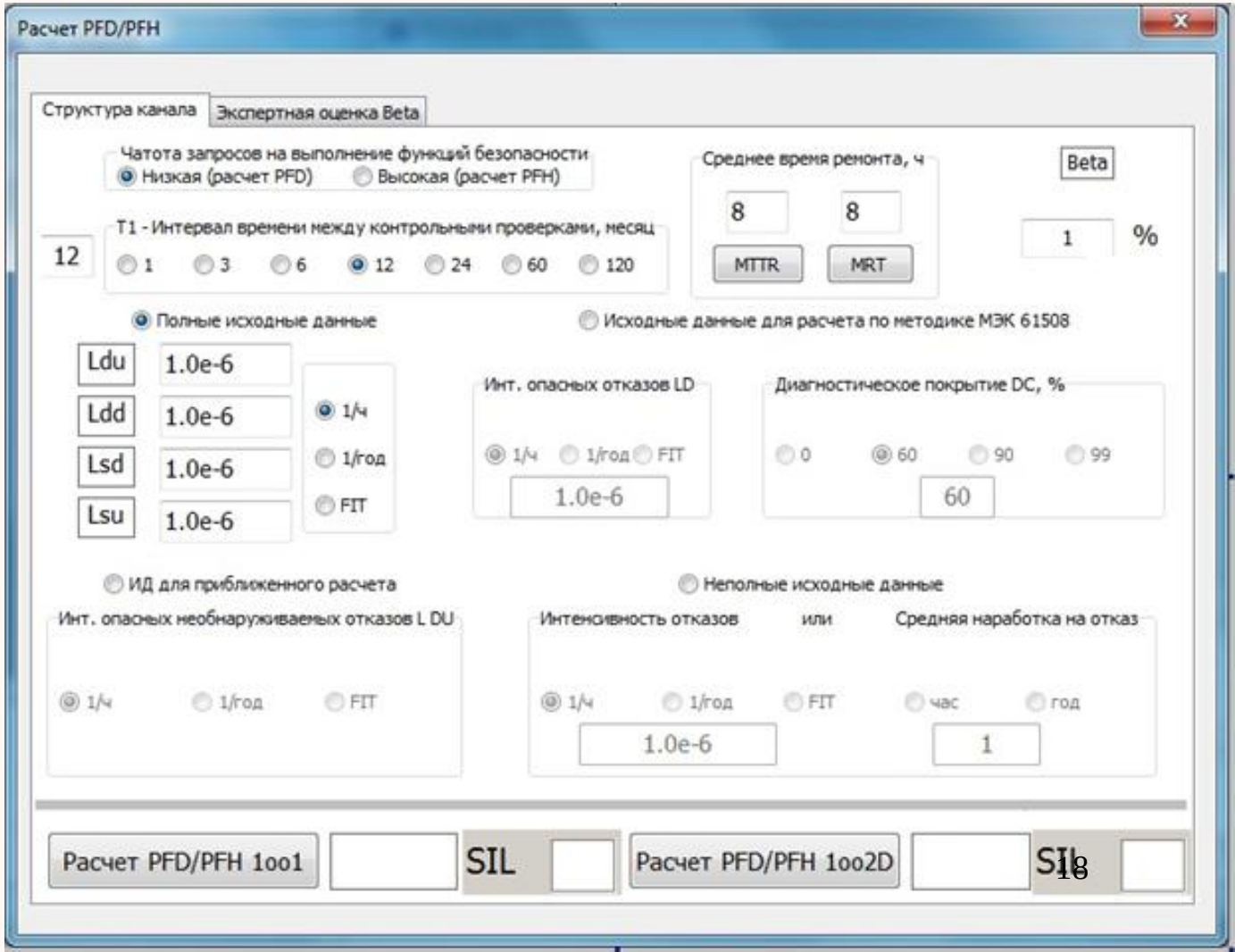
## II. ИД по компонентам канала

| Наименование элементов | $\lambda_D$, 1/ч | DC, % | β, % | $\beta_D$, % | T1, мес | MRT, ч |
|---|---|---|---|---|---|---|
| Датчики | 2.5 E-6 | 90 | 20 | 10 | 12 | 8 |
| ПЭ логические элементы | 5.0E-6 | 99 | 2 | 1 | 12 | 8 |
| Дренажный клапан | 2.5E-6 | 60 | - | - | 12 | 8 |
| Закрывающий клапан | 5.0E-6 | 60 | - | - | 12 | 8 |

## III. ИД по архитектуре элементов канала

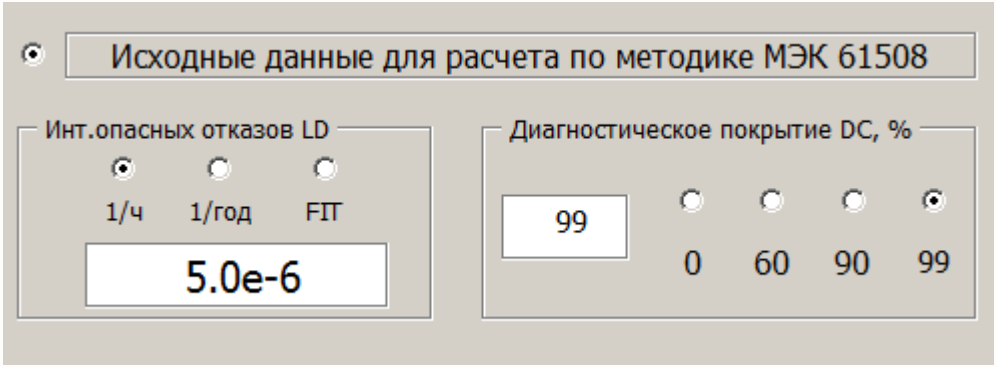
| Наименование элементов | Архитектура |
|---|---|
| Датчики | 1oo3 |
| ПЭ логические элементы | 1oo2D |
| Дренажный клапан | 2oo2 |
| Закрывающий клапан | |

# 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



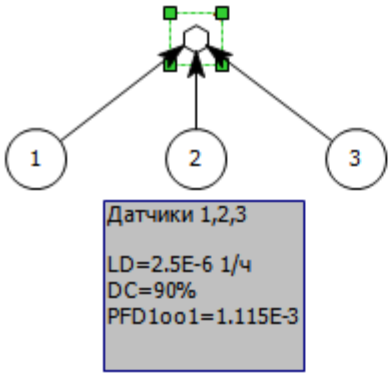
# Результаты расчета

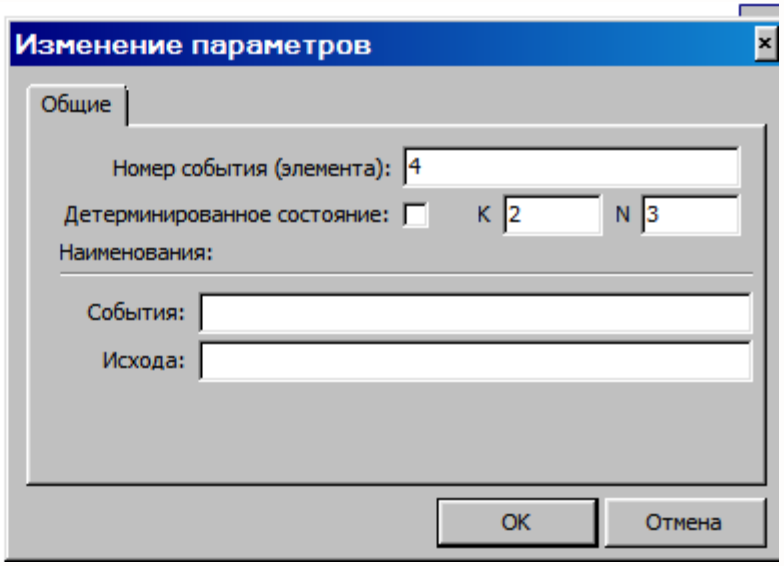
| Наименование элементов | Архитектура | PFD |
|---|---|---|
| Датчики | 1oo1 | 1.115·E-3 |
| ПЭ логические элементы | 1oo2D | 1.042·E-5 |
| Дренажный клапан | 1oo1 | 4.40·E-3 |
| Закрывающий клапан | 1oo1 | 8.80·E-3 |

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

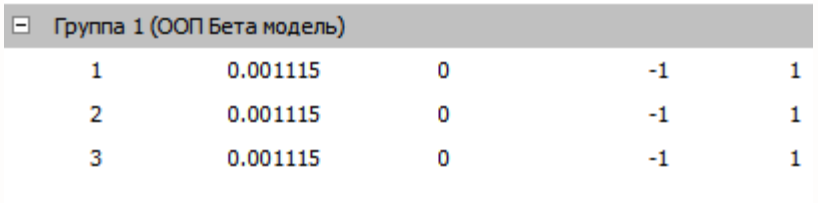
Моделирование надежности подсистемы датчиков

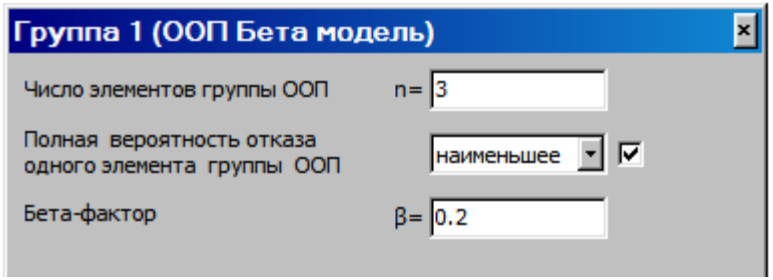
а) ДН с архитектурой 2oo3



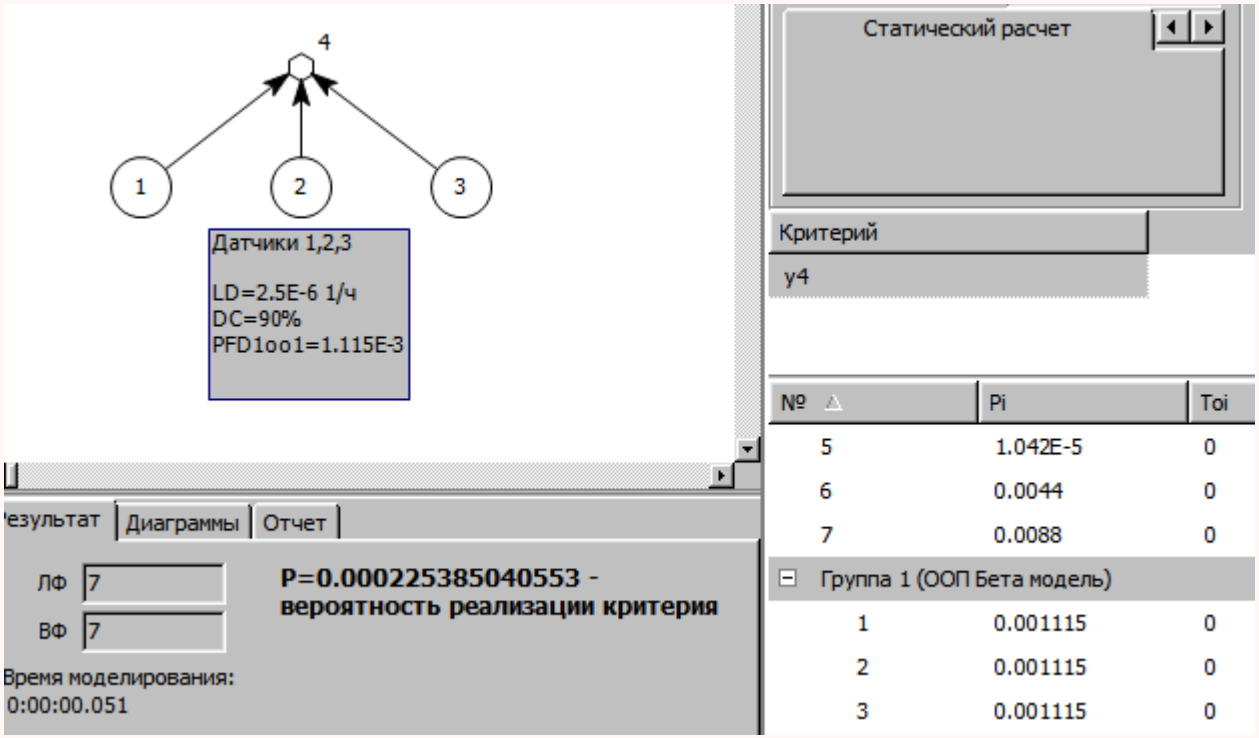




б) группа ООП



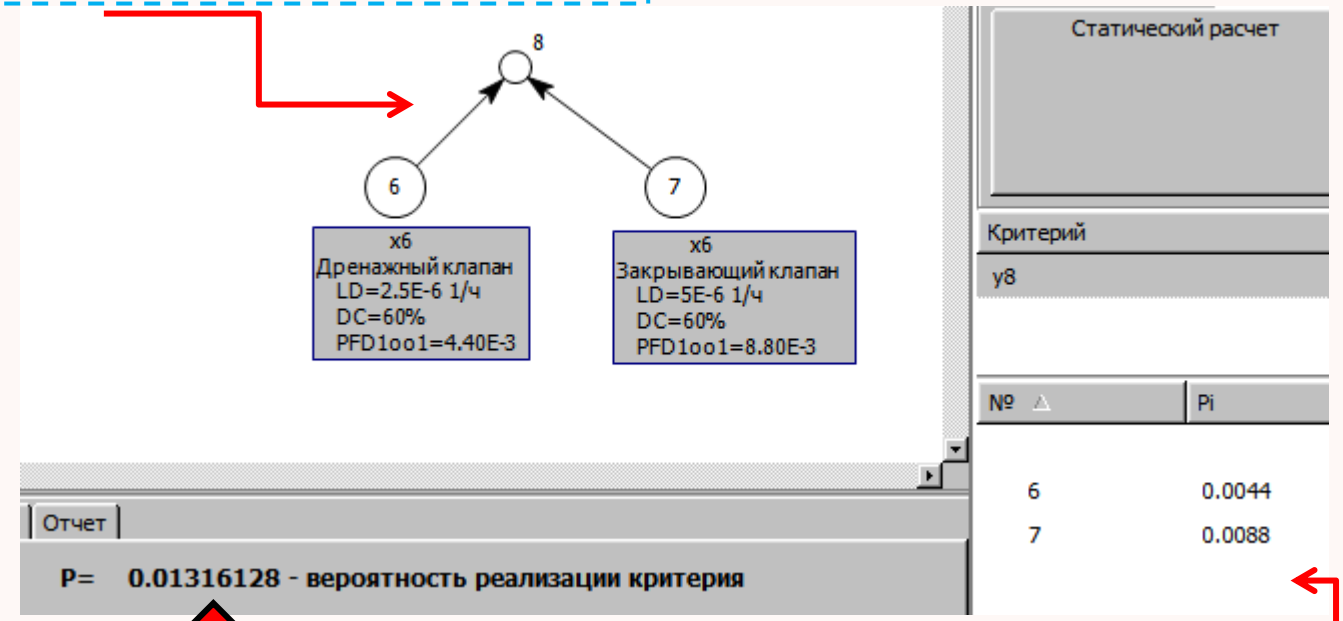



# Результаты моделирования надежности подсистемы датчиков



# Моделирование надежности подсистемы исполнительных механизмов

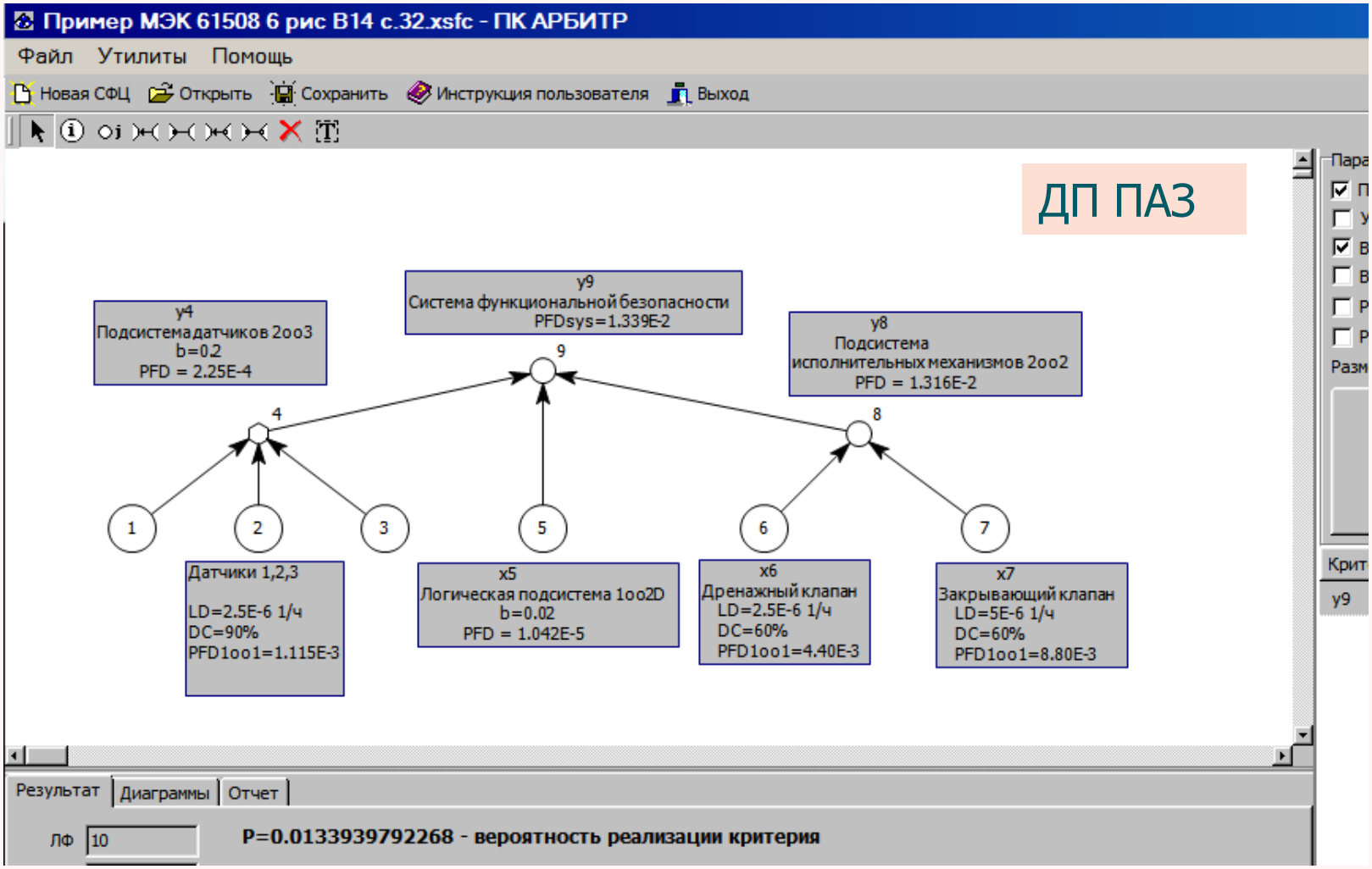
ДН исполнительных механизмов




Результаты моделирования

Исходные данные

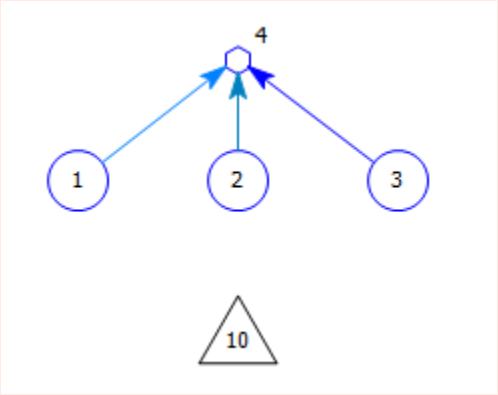
# Моделирование надежности ПАЗ



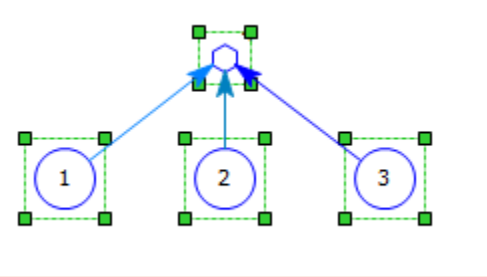

Результаты моделирования: PFD sys=1.34E-4; **SIL1**

# Формирование редуцированной СФЦ

1. Создание эквивалентированной вершины №10 для подсистемы датчиков

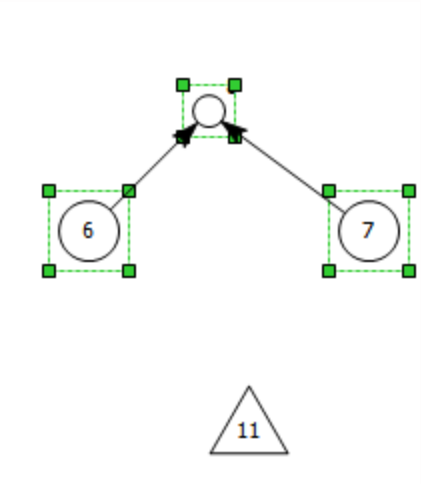



2. Копирование архитектуры подсистемы датчиков и перенос ее в вершину №10

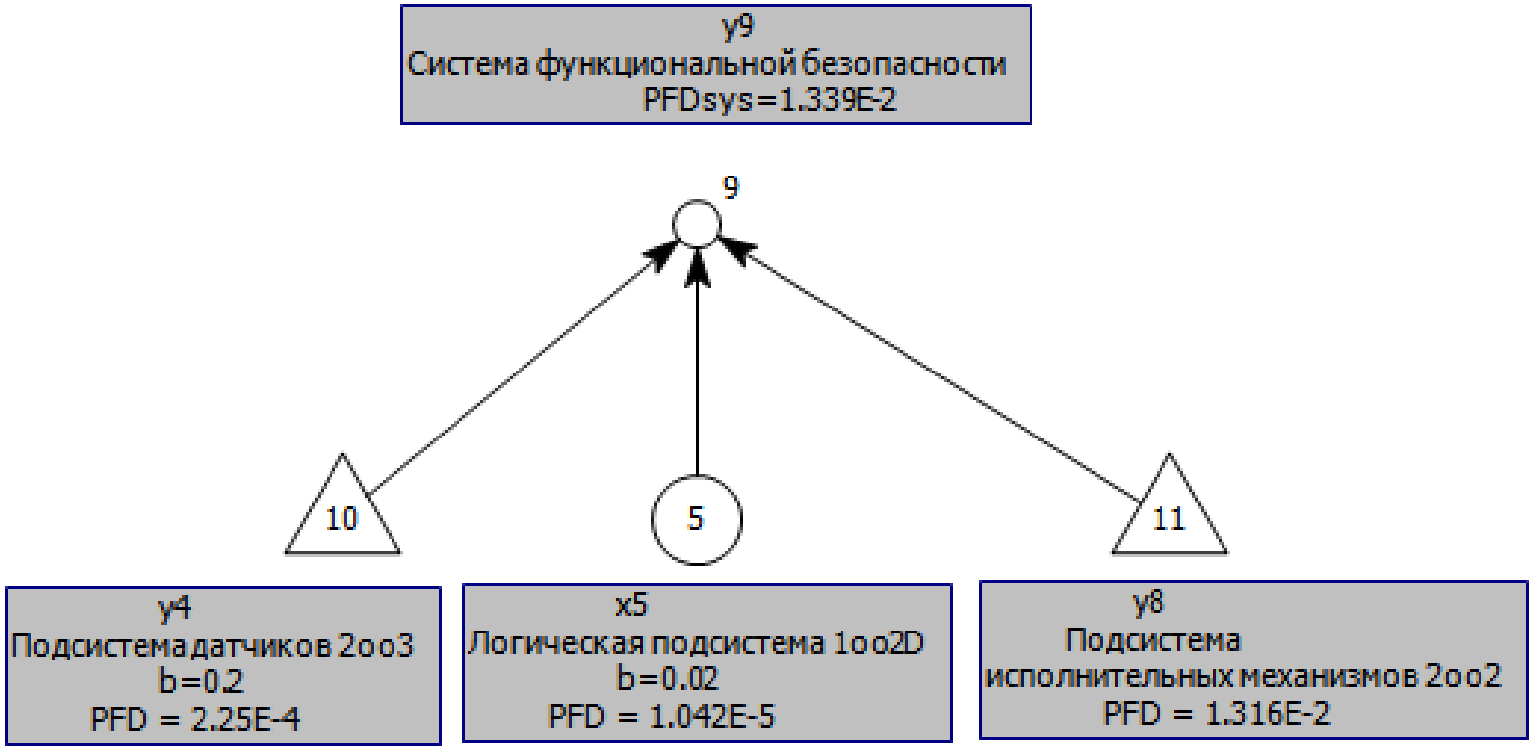


3. Создание эквивалентированной вершины №11 для подсистемы исполнительных механизмов

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



# Формирование редуцированной СФЦ



# Доклад закончен, спасибо за внимание!

Можаева Ирина Александровна

Струков Александр Владимирович

info@szma.com