УДК 681.5:004.42

М.С. Скворцов,
канд. техн. наук, вед. инженер-программист,
mikhail_skvortsov@szma.com

АО «СПИК СЗМА»,
Санкт-Петербург, Россия

Проектная оценка функциональной безопасности систем противоаварийной автоматической защиты

Проектирование систем противоаварийной автоматической защиты предусматривает выполнение требований к функциональной безопасности. Рассмотрен процесс определения достигнутых уровней полноты безопасности функциями безопасности приборных систем безопасности, разрабатываемых для предприятий перерабатывающих отраслей промышленности. Приведены примеры количественной оценки показателей функциональной безопасности систем в соответствии с рекомендациями стандартов ГОСТ Р МЭК 61508 и 61511 с помощью сертифицированного Ростехнадзором программного комплекса «АРБИТР».

Ключевые слова: функциональная безопасность, система автоматической противоаварийной защиты, уровни полноты безопасности, проектная оценка функциональной безопасности, программный комплекс «АРБИТР».
DOI: 10.24000/0409-2961-2018-1-50-57

Введение

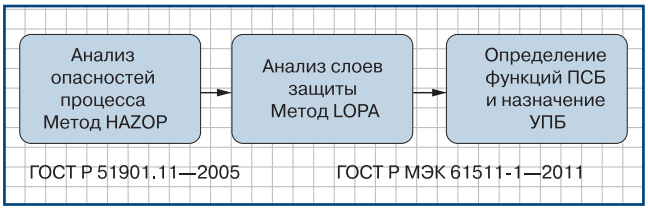
В настоящее время в Российской Федерации существует нормативная база, регламентирующая принципы построения систем безопасности опасных производственных объектов (ОПО) и требования по выбору технических средств для них. Проектирование систем противоаварийной автоматической защиты (ПАЗ) предусматривает выполнение требований, приведенных в Федеральном законе от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов» [1] и в нормативных документах Ростехнадзора. В частности, при проектировании систем ПАЗ для нефтехимических и нефтеперерабатывающих объектов следует руководствоваться Федеральными нормами и правилами в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» (далее — ФНП ОПВБ) [2].

В п. 2.1 ФНП ОПВБ [2] определено, что выбор средств контроля, управления и ПАЗ должен быть обоснован в проектной документации результатами анализа опасностей технологических процессов с использованием методов анализа риска аварий на ОПО. Кроме того, согласно п. 6.3.4 ФНП ОПВБ [2], для объектов, имеющих в своем составе блоки I и II категорий, системы ПАЗ должны создаваться на базе логических контроллеров, способных функционировать по отказобезопасной структуре и проверенных на соответствие требованиям функциональной безопасности (ФБ) систем электрических, электронных, программируемых электронных, связанных с безопасностью. Следовательно, данный пункт требует для систем ПАЗ объектов, имеющих в своем составе блоки I и II категорий, применять контроллеры, имеющие сертификат соответствия стандарту МЭК 61508.

В п. 6.3.5 ФНП ОПВБ [2] указано, что методы создания систем ПАЗ должны определяться на основании анализа опасности и работоспособности контуров безопасности с учетом риска, возникающего при отказе контура безопасности. Отметим, что требования, приведенные в пп. 2.1 и 6.3.5 ФНП ОПВБ [2], относятся к системам ПАЗ всех объектов, вне зависимости от наличия у них категории взрывоопасности. Следовательно, согласно действующей нормативной документации, проектирование систем ПАЗ должно выполняться в соответствии с результатами анализа опасностей технологического процесса, с последующей оценкой риска, связанного с возможностью отказа контура безопасности. Порядок и методы выполнения данных требований к системам ПАЗ для непрерывных производственных процессов отражены в ГОСТ Р МЭК 61511-1—2011 [3].

В ГОСТ Р МЭК 61511-1—2011 [3] понятие «функциональная безопасность» определяется как часть безопасности процесса и общей системы управления процессом, которая зависит от правильного функционирования приборной системы безопасности (ПСБ) или системы ПАЗ и других слоев защиты. Для анализа опасностей процесса стандарт предлагает использовать метод HAZOP (метод исследования опасности и работоспособности), описанный в [4, 5]. После проведения процедуры HAZOP для установленных потенциально опасных событий проводят процедуру анализа слоев защиты, которые предотвращают или снижают эту опасность (метод LOPA [6]). По результатам анализа снижения риска по каждому слою защиты определяют общую ме-

ру снижения риска и анализируют необходимость его дальнейшего снижения. Если принимается решение о необходимости дальнейшего снижения риска путем введения дополнительного слоя защиты в виде функции безопасности системы ПАЗ, то метод анализа слоев защиты позволяет определить соответствующий этой функции уровень полноты безопасности (УПБ). Данный процесс схематично представлен на рис. 1.



▲ Рис. 1. Схема формирования требований к УПБ функций безопасности ПАЗ
▲ Fig. 1. Scheme of formation of the requirements to safety integrity level of ESD safety functions

Задача оценки ФБ — изучение фактов, позволяющее судить о ФБ, достигаемой с помощью одного или более слоев защиты [4]. Данные факты устанавливаются при проверке соответствия УПБ приборных функций безопасности уровням, назначенным для них на основании процедур HAZOP (LOPA). Следовательно, оценка ФБ системы ПАЗ заключается в документальной проверке соответствия УПБ функций безопасности системы ПАЗ уровням, установленным на основании анализа опасностей и слоев защиты.

Проектную оценку ФБ можно проводить на этапе разработки проекта системы ПАЗ. Если на этапе проектирования оценка ФБ не выполнялась, то ее проведение возможно после монтажа системы на объекте и получения опыта эксплуатации и обслуживания. Рекомендуется оценивать ФБ после внесения изменений и перед выводом системы ПАЗ из эксплуатации. Для проведения проектной оценки ФБ необходимо, чтобы техническое задание на создание системы ПАЗ содержало перечень функций безопасности с назначенными УПБ.

Назначенный УПБ определяет требования к отказоустойчивости и надежности функционирования функции безопасности (контур безопасности), требования к мерам по снижению систематических отказов. Требование к отказоустойчивости определяет минимальное число отказов в контуре безопасности, при котором контур все еще может выполнять свою функцию. Другое название этих требований — структурные ограничения. Минимально допустимое число отказов приведено в табл. 1.

Требования к надежности контуров ПАЗ, в зависимости от назначенных для них УПБ, приведены в табл. 2. Для функций безопасности, работающих в режиме редких запросов, в качестве характеристики надежности контура используется средняя

Таблица 1

УПБ	Режим запросов	Минимально допустимое число отказов аппаратных средств
1	Любой	0
2	Редкие запросы	0
2	Частые (непрерывные) запросы	1
3	Любой	1
4	Любой	2

Таблица 2

УПБ	PFDavg	PFH
1	$1{\cdot}10^{-2}$–$1{\cdot}10^{-1}$	$1{\cdot}10^{-6}$–$1{\cdot}10^{-5}$
2	$1{\cdot}10^{-3}$–$1{\cdot}10^{-2}$	$1{\cdot}10^{-7}$–$1{\cdot}10^{-6}$
3	$1{\cdot}10^{-4}$–$1{\cdot}10^{-3}$	$1{\cdot}10^{-8}$–$1{\cdot}10^{-7}$
4	$1{\cdot}10^{-5}$–$1{\cdot}10^{-4}$	$1{\cdot}10^{-9}$–$1{\cdot}10^{-8}$

вероятность отказа выполнения по запросу PFD_{avg}. Для функций безопасности, работающих в режиме непрерывных запросов — средняя частота отказов в час *PFH*.

Виды отказов оборудования

Для понимания отличий между надежностью и безопасностью обратимся к классификации отказов, применяемой в ГОСТ Р МЭК 61508-6—2012 [7]. Стандарт классифицирует все отказы оборудования по следующим признакам: опасные и неопасные, обнаруженные и необнаруженные. Эти признаки в совокупности дают четыре вида отказов: опасные необнаруженные, опасные обнаруженные, безопасные обнаруженные, безопасные необнаруженные. Поэтому суммарная интенсивность отказов λ_T определяется как

$$\lambda_T = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU},$$

где λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU} — интенсивность отказов соответственно безопасных обнаруженных; безопасных необнаруженных; опасных обнаруженных; опасных необнаруженных.

Оборудование, применяемое в системах ПАЗ, обычно характеризуется высокой долей безопасных отказов и большим диагностическим охватом. Доля безопасных отказов SFF может быть вычислена как

$$SFF = (\lambda_S + \lambda_{DU})/\lambda_T,$$

где λ_S — интенсивность безопасных отказов,
а диагностический охват

$$DC = \lambda_{DD}/\lambda_D,$$

где λ_D — интенсивность опасных отказов.

В отличие от расчетов надежности системы управления процессом, в расчете показателей ФБ системы ПАЗ учитываются только опасные отказы. При этом важно, чтобы большая часть таких отказов

была диагностируема, и при их обнаружении система могла перевести процесс в безопасное состояние. Такой подход связан с тем, что безопасный отказ приводит к ложному выполнению или увеличивает вероятность ложного выполнения ФБ, переводящего управляемое оборудование или его часть в безопасное состояние. Например, в тех случаях, когда исполнительные элементы при потере питания переходят в безопасное состояние, отказы источников питания не влияют на вероятность отказа функции безопасности на запрос, поэтому такие источники питания не учитывают при расчетах PFD_{avg}. В противоположность вышесказанному опасный отказ препятствует выполнению функции безопасности, переводя управляемое оборудование в потенциально опасное состояние, или снижает вероятность корректного выполнения функции безопасности. Безопасные отказы могут быть учтены при расчетах вероятности ложного срабатывания функции безопасности.

Обычно для устройств, сертифицированных по стандарту [7], исходные данные для расчета можно найти на сайте производителя и (или) в руководстве по безопасности. Руководство по безопасности — неотъемлемая часть сертификата соответствия устройства стандарту [7], в котором указываются его УПБ и количественные характеристики отказов по типам.

Доля отказов по общей причине для избыточных структур

Требуемая отказоустойчивость функции безопасности достигается путем резервирования технических средств, которые участвуют в ее реализации. На практике, несмотря на резервирование технических средств, возникают ситуации одновременного отказа двух или более отдельных каналов многоканальной системы, приводящие к отказу функции безопасности. Поэтому для многоканальных структур стандарты по ФБ требуют учета отказов по общей причине (ООП) [8]. Это позволяет учесть возможность появления отказов, способных повлиять сразу на несколько каналов многоканальной системы. В стандарте [7] приведена методика β-фактора, с помощью которой можно определять вероятности ООП. Значения β-факторов связывают вероятность ООП с вероятностью случайного отказа. Считается, что в общее число случайных отказов оборудования включены ООП. Обычно в канале применяют диагностическое тестирование, которое обнаруживает часть отказов, поэтому общую интенсивность отказов системы, вызванную опасными ООП, вычисляют по формуле из стандарта [7]:

$$\lambda_{DU}\beta + \lambda_{DD}\beta_D, \qquad (1)$$

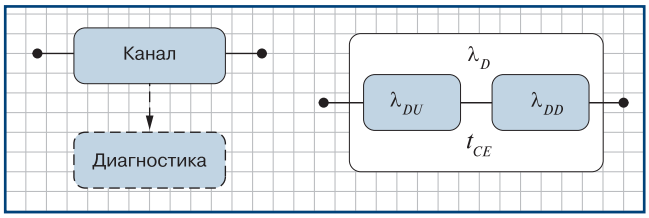
где β — фактор ООП для необнаруженных опасных отказов, который равен общему фактору, применяемому в отсутствие диагностического тестирования; β_D —доля опасных ООП, не обнаруженных диагностическими тестами. Увеличение частоты проведения диагностического тестирования приводит к уменьшению значения β_D.

Проектная оценка ФБ

Для того чтобы провести проектную оценку соответствия контуров безопасности назначенным уровням УПБ, необходимо, во-первых, убедиться, что выполнены требования, предъявляемые к отказоустойчивости контура, так называемые структурные ограничения. Во-вторых, следует убедиться, что выполнены рекомендации по снижению систематических отказов. После этого можно переходить к расчету PFD_{avg} или PFH для функции безопасности ПСБ.

Для выполнения расчета необходимы следующие исходные данные: структура контура безопасности; значения интенсивностей отказов оборудования, входящего в контур; доля ООП для избыточных структур; временной интервал между контрольными проверками оборудования контура; время ремонта и восстановления отказавшего оборудования.

Структура контура безопасности ПСБ определяет модель, по которой будут проведены расчеты PFD_{avg}. В стандарте [7] приведены блок-схемы надежности для структур 1oo1, 1oo2, 1oo2D, 2oo2, 2oo3. Блок-схема надежности для структуры 1oo1 представлена на рис. 2.



▲ Рис. 2. Структура 1oo1 и соответствующая структурная схема надежности

▲ Fig. 2. Structure 1oo1 and corresponding block-diagram of the reliability

Для данной структуры, состоящей из одного канала, любой опасный отказ приводит к нарушению функции безопасности при возникновении запроса на ее выполнение.

Стандарт [7] предлагает рассматривать канал как совокупность двух компонент: с λ_{DU}, обусловленной необнаруженными отказами, и с λ_{DD}, обусловленной обнаруженными отказами. Следовательно, суммарная интенсивность опасного отказа будет равна

$$\lambda_D = \lambda_{DU} + \lambda_{DD}.$$

В стандарте [7] для структуры 1oo1 приводятся следующие расчетные формулы:

$$PFD_{avg} = 1 - \mathbf{e}^{-\lambda_D t_{CE}} \approx \lambda_D t_{CE} = \left(\lambda_{DU} + \lambda_{DD}\right) t_{CE}; \qquad (2)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR, \qquad (3)$$

где t_{CE} — эквивалентное среднее время простоя канала; T_1 — временной интервал между контрольными проверками; MRT — среднее время ремонта; $MTTR$ — среднее время восстановления. Помимо структуры 1oo1, в стандарте [7] приведены расчетные формулы для структур 1oo2, 2oo2, 2oo3, 1oo2D.

В стандарте [7] оговаривается, что структуры систем, в нем представленные, являются примерами и не должны рассматриваться как исчерпывающие. В качестве логических методов, применимых для анализа полноты безопасности аппаратных средств ПСБ, в стандарте [7] рассмотрены блок-схемы надежности и деревья отказов. Особо отмечается, что при выборе метода расчета очень важно, чтобы аналитик был компетентен в применении метода, возможно, это даже более важно, чем сам используемый метод. Аналитик отвечает за то, чтобы гипотеза, лежащая в основе метода, была выполнена для конкретного применения, либо должна быть внесена соответствующая корректировка для достижения реалистичного консервативного результата.

Если для проведения расчетов используют программное обеспечение, то специалист, выполняющий расчет, должен понимать формулы (методы) из программного пакета, чтобы быть уверенным в том, что они применимы в данном случае. Специалист также должен проверить программный пакет путем сравнения результатов расчета нескольких тестовых примеров, полученных с помощью программного пакета и ручным способом. Таким образом, для расчетов предпочтительно использовать прошедшее проверку и аттестованное программное обеспечение, например программный комплекс «АРБИТР» (далее — ПК «АРБИТР») для автоматизированного анализа и расчета показателей надежности и безопасности структурно-сложных технических систем, который проверен независимыми экспертами и аттестован Ростехнадзором [9]. Для ПК «АРБИТР» разработаны методические рекомендации в целях проведения проектной оценки надежности [10] и безопасности.

Моделирование и расчет PFD_{avg}

Рассмотрим пример расчета PFD_{avg} для функции безопасности при помощи ПК «АРБИТР». Функция безопасности работает в режиме редких запросов. Она заключается в том, что при обнаружении превышения предельно допустимого уровня продукта в резервуаре следует перекрыть поток на вход в резервуар. Предположим, что назначенный УПБ равен 2.

Стандарты предлагают вычислять среднюю вероятность отказа по запросу для контура безопасности $PFD_к$ по формуле (4) как сумму PFD трех подсистем, образующих контур: подсистема датчиков $PFD_д$, логическая подсистема $PFD_{л.п}$ и подсистема исполнительных элементов $PFD_{и.э}$ (рис. 3).

▲ **Рис. 3. Обобщенная структурная блок-схема контура безопасности**
▲ **Fig. 3. The generalized structural block-diagram of the contour of safety**

$$PFDк \approx PFDд + PFDл.п + PFDи.э; \quad (4)$$

$$PFDк = PFDд + (1 - PFDд)PFDл.п + \\ + (1 - PFDд)(1 - PFDл.п)PFDи.э. \quad (5)$$

Следует отметить, что формула (4) является консервативным приближением, т.е. вероятность отказа на запрос при расчете по приближенной формуле получается большей, чем при расчете по точной формуле (5).

Блок-схему для расчета средней вероятности отказа на запрос представляют в ПК «АРБИТР» в виде схем функциональной целостности (СФЦ) [11, 12], которые широко применяют при моделировании и расчете надежности [13]. Построение модели для расчета PFD_{avg} выполняют при помощи пошагового последовательного уточнения с использованием метода многоуровневой структурной декомпозиции [14], реализованной в ПК «АРБИТР» с помощью эквивалентированных вершин. Эквивалентированная вершина — эквивалент (подграф) другой СФЦ. Она имеет собственную логическую структуру и служит для сокращения размерности основной СФЦ.

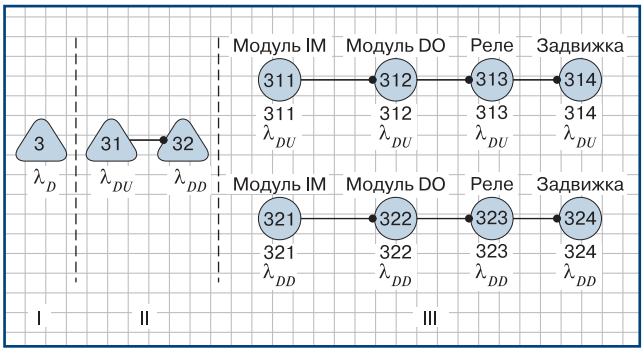
Схема функциональной целостности контура в самом общем виде представлена на рис. 4. Она состоит из трех последовательно соединенных эквивалентированных вершин, каждая из которых представляет соответствующую подсистему. Эквивалентированная вершина содержит в себе СФЦ, при помощи которой будут представлены структура и логика работы соответствующей подсистемы. Этим достигается сокращение размерности основной СФЦ и повышается наглядность.

▲ **Рис. 4. Обобщенная СФЦ**
▲ **Fig. 4. The generalized functional integrity diagram**

Рассмотрим применение метода многоуровневой структурной декомпозиции для последовательного уточнения расчетной модели каждой из подсистем.

Подсистема исполнительных элементов (структура 1оо1)

На уровне I подсистема исполнительных элементов представлена эквивалентированной вершиной 3 с суммарной интенсивностью опасных отказов $\lambda_D = \lambda_{DU} + \lambda_{DD}$ (рис. 5). На уровне декомпозиции II (внутри вершины 3) структура 1оо1 представлена, согласно стандарту [7], в виде двух элементов 31 и 32 с интенсивностью отказов λ_{DU} и λ_{DD}.

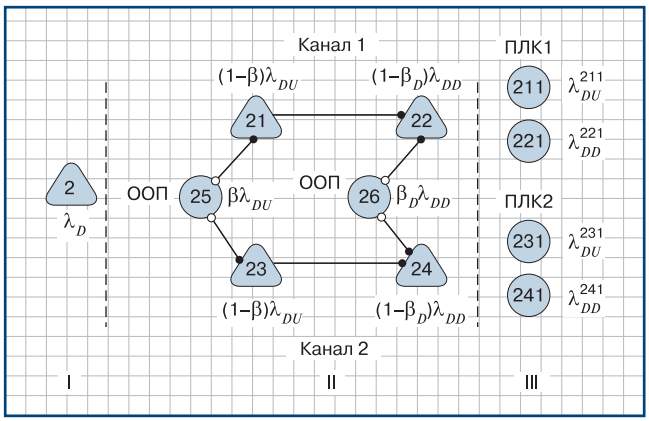


▲ **Рис. 5. Схема функциональной целостности подсистемы исполнительных элементов (структура 1оо1)**
▲ **Fig. 5. Functional integrity diagram of the subsystem of executive elements (structure 1oo1)**

На уровне декомпозиции III уточняется элементный состав канала (т.е. структура и состав эквивалентированных вершин 31 и 32) при помощи функциональных вершин графа СФЦ. Эквивалентированная вершина 31, представляющая собой необнаруженные опасные отказы канала, представлена в виде последовательного соединения функциональных вершин, которые соответствуют необнаруженным опасным отказам интерфейсного модуля IM (311), модуля дискретного выхода DO (312), реле (313) и задвижки (314). Аналогичным образом, при помощи эквивалентированной вершины 32, представляются обнаруженные опасные отказы канала (вершины 321, 322, 323, 324). Затем для вершин 311–314 и 321–324 задаются параметры для моделирования и расчета PFD_{avg} — вводятся соответствующие интенсивности, время восстановления и время между контрольными проверками. При вводе исходных данных в ПК «АРБИТР» интенсивности отказов пересчитываются в среднее время наработки между отказами (в предположении экспоненциального закона распределения) следующим образом: $MTBF = 1/\lambda_D$.

Логическая подсистема (структура 1оо2)

На уровне декомпозиции I логическая подсистема представлена эквивалентированной вершиной 2 (рис. 6). На уровне декомпозиции II (внутри вершины 2) структура 1оо2 представлена, согласно стандарту [7], в виде двух пар элементов с интенсивностью отказов λ_{DU} и λ_{DD}. Каждая пара элементов 21, 22 и 23, 24 представляет один из двух программируемых логических контроллеров (ПЛК). Вершины 25 и 26 — ООП, связанные с необнаруженными и обнаруженными опасными отказами. На уровне декомпозиции III вершины 211, 221 (231, 241) имеют структуры, вырожденные до одной вершины, параметрами которой являются интенсивности необнаруженных и обнаруженных опасных отказов ПЛК1 (ПЛК2).



▲ **Рис. 6. Схема функциональной целостности логической подсистемы (структура 1оо2)**
▲ **Fig. 6. Functional integrity diagram of the logical subsystem (structure 1oo2)**

Подсистема датчиков (структура 2оо3)

На уровне декомпозиции I подсистема датчиков представлена эквивалентированной вершиной 1 (рис. 7). На уровне декомпозиции II (внутри вершины 1) структура 2оо3 представлена, согласно стандарту [7], в виде трех пар элементов с интенсивностью отказов λ_{DU} и λ_{DD}, логика работы «два-из-трех» учтена в ПК «АРБИТР» с помощью специальной вершины «*k*-из-*n*» (вершина 9). Пары элементов 11 и 12, 13 и 14, 15 и 16 представляют каналы 1, 2 и 3 соответственно. Аналогично логической подсистеме ООП учитываются вершинами 17 и 18. На уровне декомпозиции III уточняется элементный состав каналов аналогично подсистеме исполнительных элементов.

Как видно из приведенных моделей подсистем, использование технологии многоуровневой декомпозиции, реализованной в ПК «АРБИТР», позволяет просто и наглядно представлять различные структуры подсистем для последующего анализа и расчета показателей ФБ в соответствии со стандартом [7]. Кроме этого, СФЦ на уровнях I и II являются типовыми и не зависят от конкретных технических средств реализации функции безопасности.

Исходные данные для расчета

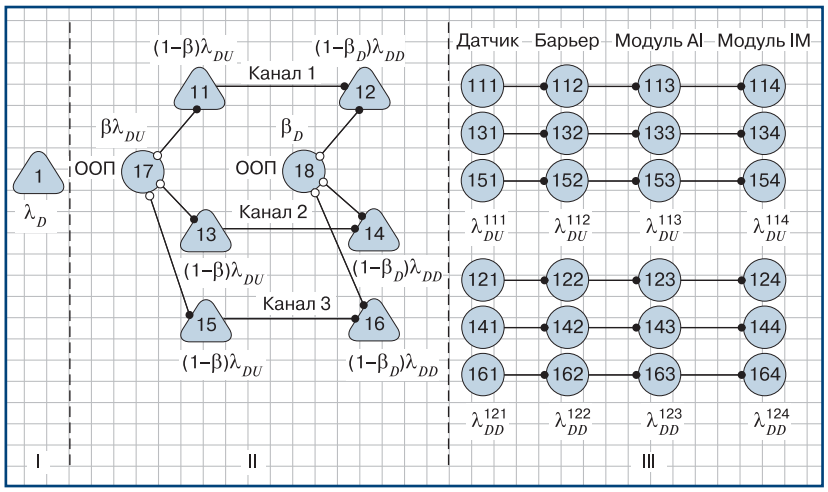
Как видно из табл. 3, моделирование и расчет показателей ФБ в ПК «АРБИТР» учитывают различия во времени восстановления $t_в$ и времени проведения контрольных проверок T_1 для элементов одного канала (одной подсистемы). Расчетные формулы, приведенные в стандарте [7], не позволяют это учитывать, так как используют предположение об одинаковом времени восстановления и одина-

ковом временном интервале между контрольными проверками для всех аппаратных средств канала. Исходные данные для расчета, представленные в табл. 3, взяты из руководств по безопасности устройств фирм Vega, MTL, Auma и др.

Результаты расчета PFD_{avg}

На рис. 8, 9 приведены результаты моделирования и расчета для каждой подсистемы и контура в целом. Моделирование и расчеты проводили для различных структур голосующих групп и различных значений β-фактора. Анализ результатов на рис. 8 (здесь *1* — структура 2oo3 ($\beta = 5$ %, $\beta_D = 10$ %); *2* — структура 2oo3 ($\beta = 1$ %, $\beta_D = 2$ %); *3* — структура 1oo2 ($\beta = 5$ %, $\beta_D = 10$ %); *4* — структура 1oo2 ($\beta = 1$ %, $\beta_D = 2$ %) показывает, что с увеличением числа ООП значения PFD_{avg} для структур 1oo2 и 2oo3 становятся очень близкими. Это подтверждает, что для избыточных структур определяющими становятся ООП. На рис. 8 видно значительное замедление роста PVD_{avg} для подсистемы исполнительных элементов для времени работы свыше 24 мес. Это связано с сильным влиянием временного интервала между контрольными проверками задвижки на общее значение PVD_{avg} подсистемы.

Используем приведенные выше результаты для расчета PFD_{avg} для следующего контура: структура подсистемы датчиков 2oo3, структура логической подсистемы 1oo2, структура подсистемы исполнительных элементов 1oo2. На рис. 9 представлены результаты расчетов подсистемы исполнительных элементов и логической подсистемы (здесь *1*, *2*, *3* — структуры подсистемы исполнительных элементов соответственно 1oo1, 1oo2 ($\beta = 5$ %, $\beta_D = 10$ %), 1oo2 ($\beta = 10$ %, $\beta_D = 20$ %); *4*, *5*, *6* — структуры логической подсистемы соответственно 1oo1, 1oo2 ($\beta = 10$ %, $\beta_D = 20$ %), 1oo2 ($\beta = 5$ %, $\beta_D = 10$ %). Для всех подсистем доля ООП составила 5 % (связаны с опасными необнаруженными отказами) и 10 % (связаны с опасными обнаруженными отказами), временной интервал между контрольными проверками — 48 мес. В соответствии с исходными данными выбираем результаты ($5{,}71 \cdot 10^{-4}$; $1{,}76 \cdot 10^{-5}$; $7{,}18 \cdot 10^{-4}$) из вышеприведенных результатов. Видно, что PFD_{avg} для каждой подсистемы лежит в интервале, который соответствует УПБ SIL 3. Отказоустойчивость контура равна 1 (определяется подсистемой контура с минимальной отказоустойчивостью), что также соответствует УПБ SIL 3. Подставляя исходные

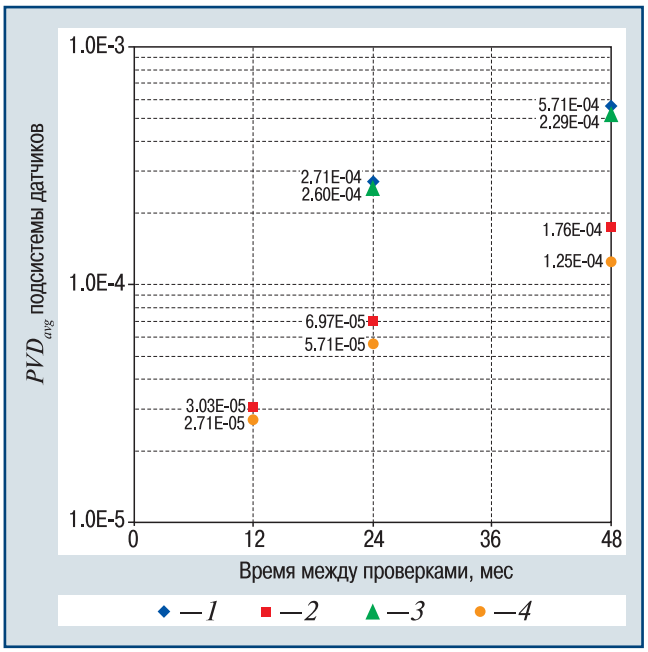


▲ **Рис. 7. Схема функциональной целостности подсистемы датчиков (структура 2oo3)**

▲ **Fig. 7. Functional integrity diagram of the subsystem of sensors (structure 2oo3)**

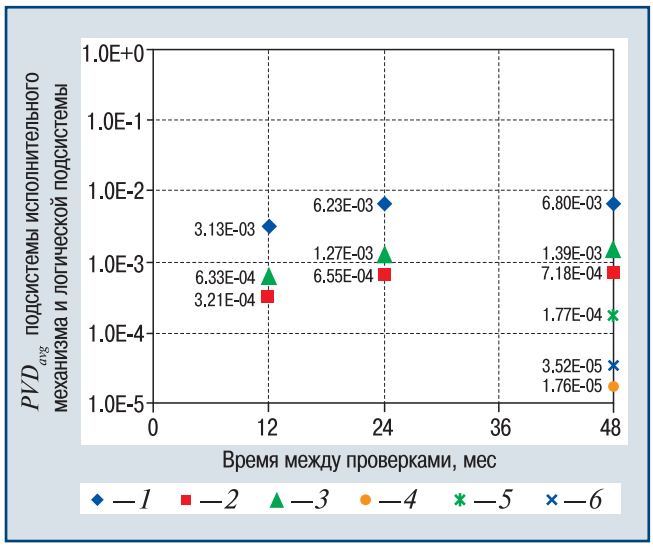
Таблица 3

Элемент контура	λ_{DD}, FIT	λ_{DU}, FIT	$t_в$, ч	T_1, мес	β_D, %	β, %
Подсистема датчика						
Датчик	990	203	8	6	10	20
Барьер	210	17	4	12	10	20
Модуль ввода аналоговый AI	388	43	4	48	10	20
Модуль интерфейсный IM	242	27	4	48	10	20
Логическая подсистема						
ПЛК	181	10	12	48	5	10
Подсистема исполнительных элементов						
Модуль интерфейсный IM	242	27	4	48	—	—
Модуль вывода дискретный DO	304	34	4	48	—	—
Реле	96	3,6	4	48	—	—
Задвижка	367	647	24	24	—	—



▲ **Рис. 8. Результаты расчетов подсистемы датчиков**

▲ **Fig. 8. The results of calculations of the subsystem of sensors**



▲ **Рис. 9. Результаты расчетов подсистемы исполнительных элементов и логической подсистемы**
▲ **Fig. 9. The results of calculations of the subsystem of executive elements and logical subsystem**

данные в формулу (5), получаем результирующую $PFD_{avg} = 1{,}31 \cdot 10^{-3}$, что соответствует УПБ SIL 2. Таким образом, только проведение расчета значения PFD_{avg} для всего контура может гарантировать определение достигнутого им УПБ. Даже если каждая из подсистем соответствует УПБ SIL 3, то результирующий УПБ контура может быть равен SIL 2.

Выводы

1. Существующая нормативно-правовая база предписывает необходимость выполнения требований стандартов по анализу опасностей и риска аварий и обеспечению ФБ систем ПАЗ на ОПО. Поэтому в состав проектной (рабочей) документации на строительство, реконструкцию и техническое перевооружение и другие виды строительства ОПО необходимо включать следующие документы:

отчет о проведении анализа опасностей и работоспособности, включающий результаты проведения процедуры HAZOP;

отчет о назначении УПБ для функций системы ПАЗ, включающий результаты проведения процедуры SIL-анализа, предусматривающей анализ выявленных рисков, распределение риска по слоям защиты, определение перечня функций (контуров) системы ПАЗ и назначение для каждого из них УПБ;

проектную оценку ФБ, содержащую подтверждение соответствия характеристик ФБ контуров системы ПАЗ характеристикам, соответствующим назначенным для них УПБ. При этом для указанного подтверждения должны быть построены адекватные функциональные модели контуров безопасности и, согласно моделям, выполнены расчеты фактических вероятностных показателей ФБ этих контуров. Для обеспечения корректной разработки данного документа проектными организациями следует выпустить соответствующий руководящий документ, содержащий необходимые методические указания.

Для безусловного выполнения вышеуказанных требований стандартов необходимо выпустить нормативные акты, предписывающие включение данных документов в состав документации на ОПО, предоставляемой на государственную экспертизу и экспертизу промышленной безопасности.

2. Приведена опробованная методика расчета PFD_{avg} для функций безопасности систем ПАЗ. В основе методики лежат методы автоматизированного структурно-логического моделирования и многоуровневой структурной декомпозиции. Расчет PFD_{avg} — важная часть подтверждения соответствия функций безопасности назначенным УПБ.

3. Для расчета показателей ФБ предлагается использовать отечественный ПК «АРБИТР», сертифицированный Ростехнадзором и предназначенный для моделирования и расчета надежности и безопасности структурно-сложных систем, включая объекты использования атомной энергии и другие ОПО.

Список литературы

1. *О промышленной* безопасности опасных производственных объектов: федер. закон от 21 июля 1997 г. № 116-ФЗ. — М.: ЗАО НТЦ ПБ, 2017. — 52 с.

2. *Общие* правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств: федер. нормы и правила в обл. пром. безопасности. — Сер. 09. — Вып. 37. — М.: ЗАО НТЦ ПБ, 2016. — 127 с.

3. *ГОСТ Р МЭК 61511-1—2011.* Безопасность функциональная. Системы безопасности приборные для промышленных процессов. — М.: Стандартинформ, 2012. — 67 с.

4. *ГОСТ Р 51901.11—2005* (МЭК 61882:2001). Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство. — М.: Стандартинформ, 2005. — 43 с.

5. *Tyler B., Crawley F.* HAZOP: Guide to Best Practice. — Elsevier, 2015. — 168 p.

6. *Basu S.* Plant hazard analysis and safety instrumentation systems. — Elsevier, 2017. — P. 346–370.

7. *ГОСТ Р МЭК 61508-6—2012.* Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 6. — М.: Стандартинформ, 2014. — 104 с.

8. *Rausand M., Houland A.* System reliability theory: models, statistical methods, and applications. — John Wiley&Sons, 2009. — P. 442–446.

9. *Можаев А.С.* Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА)// Вопросы атомной науки и техники. Сер. «Физика ядерных реакторов». — 2008. — Вып. 2. — С. 105–116.

10. *Методические* рекомендации. Автоматизированные системы управления. Надежность и безопасность. Расчет надежности и безопасности автоматизированных систем управления технологическими процессами и инженерным

оборудованием на стадии проектировании. — М.: ОАО Ассоциация «Монтажавтоматика», 2011. — 33 с.

11. *Можаев А.С.* Универсальный графоаналитический метод, алгоритм и программный модуль построения монотонных и немонотонных логических функций работоспособности систем// Тр. Междунар. науч. шк. «Моделирование и анализ безопасности, риска в сложных системах». — СПб: СПбГУАП, 2003. — С. 101–110.

12. *Технология* автоматизированного моделирования структурно-сложных систем/ И.А. Рябинин, А.С. Можаев, С.К. Свирин, В.И. Поленин// Морская радиоэлектроника. — 2007. — № 1. — С. 52–55.

13. *Можаев А.С., Скворцов М.С., Струков А.В.* Применение автоматизированного структурно-логического моделирования для проектного расчета надежности АСУ// Нефть. Газ. Новации. — 2010. — № 9. — С. 72–78.

14. *Применение* ПК «АРБИТР» в задачах проектной оценки надежности структурно-сложных систем/ И.А. Гладкова, А.С. Можаев, А.А. Нозик, А.В. Струков// Сб. докл. Междунар. науч. семинара им. Ю.Н. Руденко «Методические вопросы исследования надежности больших систем энергетики». — Иркутск, 2015.

mikhail_skvortsov@szma.com

Материал поступил в редакцию 25 октября 2017 г.

«Bezopasnost Truda v Promyshlennosti»/ «Occupational Safety in Industry», 2018, № 1, pp. 50–57.
DOI: 10.24000/0409-2961-2018-1-50-57

Design Assessment of Functional Safety of Emergency Shutdown System

Information about the Author
M.S. Skvortsov, Cand. Sci. (Eng.), Lead Software Engineer, mikhail_skvortsov@szma.com
AO «SPIK SZMA», Saint-Petersburg, Russia

Abstract
At present in the Russian Federation there is the regulatory base regulating the principles of creation of safety systems for hazardous production facilities, and the requirements for selecting technical means for them. Design of emergency shutdown systems provides for the fulfillment of the requirements of functional safety. The requirements of standards for functional safety are provided to reliability and fault tolerance of contours of safety of emergency shutdown systems. The methods are described concerning the application of functional integrity diagrams for creation of structural and logical models for calculation of indicators of reliability for contours of emergency shutdown systems. The process is considered related to identification of the reached levels of safety by functions of safety of emergency shutdown systems developed for the enterprises of processing industries. The list of documents is given, which should be included in to the scope of design (working) documentation for construction, reconstruction and technical-re-equipment. Examples are shown concerning the quantitative assessment of indicators of functional safety of the systems according to the recommendations of standards GOST R IEC 61508-6—2012 and GOST R IEC 61511-1—2011 by means of the ARBITR software complex certified by Rostechnadzor. The conclusion is drawn on the need in including the design assessment of functional safety in the scope of documentation submitted for state expertise and for industrial safety expertise.

Key words: functional safety, emergency shutdown system, levels of completeness of safety, design assessment of functional safety, ARBITR software complex.

References

1. *O promyshlennoj bezopasnosti opasnyh proizvodstvennyh obektov: feder. zakon ot 21 ijulja 1997 g. № 116-FZ* (On Industrial Safety of Hazardous Production Facilities: Federal Law of July 21, 1997 № 116-FL). Moscow: ZAO NTTs PB, 2017. 52 p.

2. *Obshhie pravila vzryvobezopasnosti dlja vzryvopozharoopasnyh himicheskih, neftehimicheskih i neftepererabatyvajushhih proizvodstv: feder. normy i pravila v obl. prom. Bezopasnosti* (General Rules of Explosion Safety for Fire and Explosion and Fire Hazardous Chemical, Petrochemical and Oil Refineries: Federal Norms and Rules in the Field of Industrial Safety). Ser. 09. Iss. 37. Moscow: ZAO NTTs PB, 2016. 127 p.

3. *GOST R MEK 61511-1—2011. Bezopasnost funktsionalnaya. Sistemy bezopasnosti pribornye dlya promyshlennykh protsessov* (GOST R IEC 61511-1—2011. Functional Safety. Safety Instrumentation Systems for Industrial Processes). Moscow: Standartinform, 2012. 67 p.

4. *GOST R 51901.11—2005 (MEK 61882:2001). Menedzhment riska. Issledovanie opasnosti i rabotosposobnosti. Prikladnoe rukovodstvo* (GOST R 51901.11—2005 (IEC 61882:2001). Risk Management. Study of Hazard and Operability. Practicable Guidelines). Moscow: Standartinform, 2005. 43 p.

5. Tyler B., Crawley F. HAZOP: Guide to Best Practice. Elsevier, 2015. 168 p.

6. Basu S. Plant hazard analysis and safety instrumentation systems. Elsevier, 2017. pp. 346–370.

7. *GOST R MEK 61508-6—2012. Funktsionalnaya bezopasnost sistem elektricheskikh, elektronnykh, programmiruemykh elektronnykh, svyazannykh s bezopasnostyu. Chast 6* (GOST R IEC 61508-6—2012. Functional Safety of the Electric, Electronic, Programmable Electronic Related to Safety Systems. Part 6). Moscow: Standartinform, 2014. 104 p.

8. Rausand M., Houland A. System reliability theory: models, statistical methods, and applications. John Wiley&Sons, 2009. pp. 442–446.

9. Mozhaev A.S. Summary of the software ARBITR (ASM SZMA). *Voprosy atomnoy nauki i tekhniki. Ser. «Fizika yadernykh reaktorov» = Issues Related to Nuclear Science and Technology. Series «Physics of Nuclear Reactors»*. 2008. Iss. 2. pp. 105–116.

10. *Metodicheskie rekomendatsii. Avtomatizirovannye sistemy upravleniya. Nadezhnost i bezopasnost. Raschet nadezhnosti i bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami i inzhenernym oborudovaniem na stadii proektirovanii* (Methodical Recommendations. Distributed Control Systems. Reliability and Safety. Calculation of Reliability and Safety of DCS for Process and Engineering Equipment at the Stage Design Stage). Moscow: OAO Assotsiatsiya «Montazhavtomatika», 2011. 33 p.

11. Mozhaev A.S. Universal graphic-analytical method, algorithm and software module of creation of monotonous and nonmonotonic logical functions of systems operability. *Tr. Mezhdunar. nauch. shk. «Modelirovanie i analiz bezopasnosti, riska v slozhnykh sistemakh» = Proceedings of the International Scientific School «Modeling and Analysis of Safety, Risk in the Complicated Systems»*. Saint-Petersburg: SPbGUAP, 2003. pp. 101–110.

12. Ryabinin I.A., Mozhaev A.S., Svirin S.K., Polenin V.I. Technology of the automated modeling of structural and complicated systems. *Morskaya radioelektronika = Sea Radioelectronics*. 2007. № 1. pp. 52–55.

13. Mozhaev A.S., Skvortsov M.S., Strukov A.V. Application of the automated structural and logical modeling for design calculation of DCS reliability. *Neft. Gaz. Novatsii = Oil. Gas. Innovations*. 2010. № 9. pp. 72–78.

14. Gladkova I.A., Mozhaev A.S., Nozik A.A., Strukov A.V. Use of the ARBITR personal computer in the tasks of design assessment of reliability of the structural and complicated systems. *Sb. dokl. Mezhdunar. nauch. seminara im. Yu.N. Rudenko «Metodicheskie voprosy issledovaniya nadezhnosti bolshikh sistem energetiki» = Book of Reports of the International Seminar of Yu.N. Rudenko «Methodical Issues of Study of the Reliability of Large Energy Systems»*. Irkutsk, 2015.