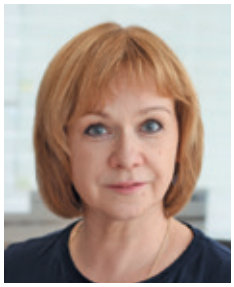
Особенности оценки показателей функциональной безопасности систем противоаварийной автоматической защиты с использованием деревьев неисправностей

Specificity of fault tree-based functional safety indicator definition in emergency shutdown systems

Можаева И.А.[1]*, Струков А.В.[1]
Mozhaeva I.A.[1]*, Strukov A.V.[1]

[1]Общество с ограниченной ответственностью «Специализированная инжиниринговая компания Севзапмонтажавтоматика» (ООО «СПИК СЗМА»)
[1]SPIK SZMA
**irina_mozhaeva@szma.com*



Можаева И.А.

Струков А.В.

Резюме. Цель. *Целью статьи является анализ особенностей использования коммерческих программных пакетов, основанных на моделях деревьев неисправностей (ДН), которые применяются в инженерной практике для расчета надежности систем противоаварийной автоматической защиты (ПАЗ). Стандарты серии МЭК 61508 «Функциональная безопасность» обращают внимание на возможность получения в таких случаях неверных и неконсервативных оценок средней вероятности отказа на запрос выполнения функций безопасности ПАЗ. Основным источником некорректных результатов является применение приближенных и упрощенных формул для определения показателей надежности компонентов контуров ПАЗ, и вычисление показателя средней неготовности системы ПАЗ к выполнению функций безопасности по значениям средней неготовности ее компонентов. Для коррекции результатов моделирования ДН возможно использование поправочных коэффициентов, учитывающих структуру контура ПАЗ, а также применение точных формул стандарта МЭК 61508-6 для расчета средней вероятности отказа на запрос компонентов контура ПАЗ. Кроме того, возможен выбор типа модели отказов по общим причинам (ООП).* **Методы.** *Проведен сравнительный анализ влияния составляющих опасных отказов, обнаруживаемых и не обнаруживаемых внутренним диагностированием, на оценку средней вероятности отказа на запрос компонентов контура ПАЗ. Показано, что для менее надежных компонентов эта зависимость существенно влияет на занижение оценки показателя неготовности. Эффективность введения корректирующих коэффициентов, учитывающих архитектуру контура ПАЗ, также зависит от надежности компонентов, и их введение целесообразно для тех компонентов, чей уровень полноты безопасности соответствует диапазону между уровнями 1 и 2. Для проектной оценки показателей функциональной безопасности возможно применение модели бета-фактора отказов по общим причинам, применяемой при проектном расчете функциональной безопасности ПАЗ.* **Результаты**. *Анализ упрощенных и приближенных формул для расчета средней неготовности нерезервированных элементов контура ПАЗ показал, что при диагностическом покрытии более 90% использование упрощенных формул приводит к занижению показателя неготовности за счет увеличения влияния опасных обнаруженных отказов на вероятность несрабатывания ПАЗ. При использовании метода анализа ДН для получения консервативной оценки показателя неготовности контура ПАЗ следует использовать корректирующие коэффициенты, значения которых зависят от параметров резервирования каналов ПАЗ. Рассмотрены две модели учета ООП, применяемые при расчетах функциональной безопасности ПАЗ. Показано, что при использовании любой модели ООП показатели надежности системы снижаются. Это снижение определяется величиной бета-фактора и надежностью элементов системы ПАЗ.* **Заключение.** *Изложенные в статье материалы показывают ограничения применения упрощенной формулы для оценки средней неготовности нерезервированных элементов ПАЗ в качестве исходных данных для построения ДН. При определении уровня полноты безопасности контура ПАЗ, имеющего в своем составе элементы с низкой надежностью, следует учитывать, что при использовании метода ДН в коммерческих программных пакетах возможно получение завышенных показателей надежности, что нежелательно в задачах анализа функциональной безопасности.*

Abstract. Aim. *The paper aims to analyse the specifics of the use of commercial fault tree (FT)-based software suites as part of engineering practice for the purpose of dependability calculation of emergency shutdown systems (ESS). Standards of the IEC 61508 Functional safety series stress that, in such cases, there is a possibility of incorrect and non-conservative*

estimates of the mean probability of failure on demand of an ESS safety feature. Incorrect results are primarily caused by the use of approximate and simplified formulas for identifying the dependability indicators of ESS circuit components and calculating the ESS mean unavailability for safety function performance based on the mean unavailability values of its components. In order to correct the FT simulation results, correction factors can be used that take into account the ESS circuit structure along with exact formulas per IEC 61508-6 for calculating the mean probability of failure on demand of the ESS circuit components. Additionally, the type of common cause failure (CCF) model can be chosen. **Methods.** *A comparative analysis was performed as regards the effects of components of hazardous failures that may be detected or not detected by internal diagnostics on the assessment of the mean probability of failure on demand of an ESS circuit components. It was shown that in less dependable components this dependence significantly affects the unavailability value. The efficiency of correction coefficients that take into account the ESS circuit architecture also depends on the dependability of components, and their introduction is justified for those components whose safety integrity level is between 1 and 2. Engineering estimation of the functional safety indicators can be done using a beta-factor model of common cause failures that is employed as part of design analysis of ESS functional safety.* **Results.** *An analysis of simplified and approximate formulas for calculating the mean unavailability of the non-redundant elements of an ESS circuit has shown that in the case of an over 90-percent diagnostic coverage the use of simplified formulas causes an underestimation of the unavailability indicator caused by the increased effect of detected hazardous failures on the probability of ESS misoperation. If the FT analysis is used for the purpose of deducing a conservative estimate of an ESS circuit unavailability indicator, correction factors should be used, whose values depend on the ESS channels redundancy parameters. Two models of accounting for CCF were examined that are used when calculating ESS functional safety. It was shown that under any ESS model the system's dependability indicators decrease. This decrease is defined by the value of the beta factor and the dependability of the ESS system elements.* **Conclusion.** *The information presented in the paper indicates the limited applicability of the simplified formula for calculating the mean unavailability of non-redundant ESS elements as the input data for FT construction. When identifying the safety integrity level of an ESS circuit that includes elements with a low dependability, it should be taken into consideration that, if a FT is used, commercial software suites may overestimate the dependability, which is undesirable in respect to functional safety analysis.*

Ключевые слова: *надежность, функциональная безопасность, система противоаварийной автоматической защиты, отказы по общим причинам, дерево неисправностей.*
Keywords: *dependability, functional safety, emergency shutdown system, common cause failures, fault tree*

Для цитирования: *Можаева И.А., Струков А.В. Особенности оценки показателей функциональной безопасности систем противоаварийной автоматической защиты с использованием деревьев неисправностей // Надежность. 2022. №4. С. 45-52. https://doi.org/10.21683/1729-2646-2022-22-4-45-52*
For citation: *Mozhaeva I.A., Strukov A.V. Specificity of fault tree-based functional safety indicator definition of emergency shutdown systems. Dependability 2022;4:45-52. https://doi.org/10.21683/1729-2646-2022-22-4-45-52*

Поступила 19.08.2022 / **После доработки** 21.10.2022 / **К печати** 15.12.2022
Received on: 19.08.2022 / **Revised on:** 21.10.2022 / **For printing:** 15.12.2022.

Введение

Показатели функциональной безопасности систем противоаварийной автоматической защиты (ПАЗ) являются показателями надежности восстанавливаемых систем, работающих в режиме запроса. Так, например, основной показатель функциональной безопасности, определяющий уровень полноты безопасности контуров ПАЗ, – средняя вероятность отказа на запрос *PFDavg* – есть средняя неготовность ПАЗ на интервале между контрольными проверками. Использование приближенных или упрощенных формул для расчета показателя *PFDavg* может привести к ошибочным выводам.

В приложении *B* стандарта МЭК 61508-6-2012 [1] отмечаются две причины, которые могут привести к неверным, неконсервативным оценкам надежности систем ПАЗ, которые нежелательны при обеспечении безопасности промышленных процессов. Первая причина связана с использованием упрощенных формул оценки средней неготовности *PFDavg i* – средней вероятности отказа на запрос *i*-го компонента системы ПАЗ. Вторая причина связана с тем, что для избыточных структур невозможно получить оценку средней неготовности системы ПАЗ только путем объединения обычным способом значений *PFDavg i* ее компонентов. С математической точки зрения это объясняется

тем, что произведение средних не всегда есть среднее произведений.

В этой связи важным является понимание инженерами, проводящими расчет надежности систем ПАЗ с использованием коммерческих программных пакетов, основанных на использовании моделей дерева неисправностей (ДН), причин и размера ошибок, допускаемых при расчетах.

Упрощенные и приближенные формулы для нерезервированных элементов

Упрощенные формулы для расчета *PFDavg* были введены в работе M. Rausand [2]. Формулы просты в использовании и дают адекватные результаты для многих архитектур каналов систем ПАЗ при определенных исходных данных о надежности компонентов и условиях эксплуатации.

Для архитектуры 1oo1, в которой любой опасный отказ приводит к отказу функции безопасности при обращении к ней, упрощенная формула для расчета показателя *PFDavg* имеет вид

$$PFD_{avg} \cong \frac{1}{2}\lambda_{du} TI, \qquad (1)$$

где $\lambda_{du} = \lambda_D(1-\frac{DC}{100})$ – интенсивность опасных (*dangerous*) необнаруженных (*undetected*) отказов;

λ_D – интенсивность опасных отказов;

TI – интервал между контрольными проверками (*proof Test Interval*);

DC – диагностическое покрытие (достоверность диагностирования опасных отказов).

В упрощенной формуле учитываются только опасные необнаруженные отказы (*DU*). Также в упрощенных формулах среднее время восстановления (*MTTR*) и среднее время ремонта (*MRT*) считаются пренебрежительно малыми по сравнению с межконтрольным интервалом *TI*. Анализ влияния опасных обнаруженных отказов и ненулевого времени восстановления или ремонта можно показать на примерах расчета *PFDavg* для архитектуры 1oo1 для крайних значений интенсивности опасных отказов λ_D $2{,}5\cdot10^{-5}$ 1/ч и $5\cdot10^{-8}$ 1/ч, диагностического покрытия *DC* и межконтрольных интервалов *TI*, приведенных в таблицах приложения *B* стандарта МЭК 61508-6 [1].

В [1] приводятся приближенные формулы для расчета средней вероятности отказов на запрос, полученные на основе марковских моделей и пригодные для инженерного использования [3, 7]. Согласно стандарту [1] значение *PFDavg* для архитектуры 1oo1 рассчитывается по формуле

$$PFD_{avg\ 1oo1} = \frac{1}{2}\lambda_{du}\left(TI + MTTR\right) + \lambda_{dd} MRT, \qquad (2)$$

где $\lambda_{dd} = \lambda_D \frac{DC}{100}$ – интенсивность опасных (*dangerous*) обнаруженных (*detected*) отказов.

В табл. 1 показано влияние доли опасных обнаруженных и необнаруженных отказов при диагностическом покрытии 99% и 90% на показатель *PFDavg* для архитектуры 1oo1 при различных значениях интервала между контрольными проверками *TI*.

Значения среднего времени восстановления и среднего времени ремонта выбраны, как и в МЭК 61508-6, равными *MTTR* = *MRT* = 8 час.

Как видно из табл. 1, заметное влияние опасных обнаруженных отказов имеет место только при значениях диагностического покрытия *DC* > 90%.

Повышение доли опасных обнаруженных отказов в общем потоке опасных отказов, что определяется значением показателя *DC*, приводит к получению заниженных оценок по формуле (1). Так, при *TI* = 4380 ч., $\lambda_D = 5\cdot10^{-8}$ (1/ч) и *DC* = 99%

по формуле (1):

$$PFD_{avg1oo1} = \frac{1}{2}\lambda_{du} TI =$$

$$= \frac{1}{2}\cdot 5{,}00\cdot10^{-10}\cdot 4380 = 1{,}095\cdot10^{-6},$$

по формуле (2):

$$PFD_{avg1oo1} = \frac{1}{2}\lambda_{du}\left(TI + MTTR\right) + \lambda_{dd} MTR =$$

$$= \frac{1}{2}5{,}00\cdot10^{-10}\cdot\left(4380+8\right) +$$

$$+4{,}95\cdot10^{-8}\cdot 8 = 1{,}493\cdot10^{-6}.$$

Таблица 1 – Влияние опасных обнаруженных и необнаруженных отказов на показатель *PFDavg* для архитектуры 1oo1

DC	***TI* = 6 месяцев**	***TI* = 120 месяцев**
99%	$\lambda_D = 2{,}5\cdot10^{-5}$, $\lambda_{DU} = 2{,}5\cdot10^{-7}$, $\lambda_{DD} = 2{,}475\cdot10^{-5}$	$\lambda_D = 5\cdot10^{-8}$, $\lambda_{DU} = 5\cdot10^{-10}$, $\lambda_{DD} = 4{,}95\cdot10^{-5}$
	$PFD_{avg} = \underbrace{\frac{1}{2}\lambda_{du}\left(TI+MTTR\right)}_{73{,}476\%} + \underbrace{\lambda_{dd} MTR}_{26{,}524\%}$	$PFD_{avg} = \underbrace{\frac{1}{2}\lambda_{du}\left(TI+MTTR\right)}_{98{,}2\%} + \underbrace{\lambda_{dd} MTR}_{1{,}8\%}$
90%	$\lambda_D = 2{,}5\cdot10^{-5}$, $\lambda_{DU} = 2{,}5\cdot10^{-6}$, $\lambda_{DD} = 2{,}25\cdot10^{-5}$	$\lambda_D = 5\cdot10^{-8}$, $\lambda_{DU} = 5\cdot10^{-9}$, $\lambda_{DD} = 4{,}5\cdot10^{-8}$
	$PFD_{avg} = \underbrace{\frac{1}{2}\lambda_{du}\left(TI+MTTR\right)}_{96{,}8\%} + \underbrace{\lambda_{dd} MTR}_{3{,}2\%}$	$PFD_{avg} = \underbrace{\frac{1}{2}\lambda_{du}\left(TI+MTTR\right)}_{99{,}8\%} + \underbrace{\lambda_{dd} MTR}_{0{,}2\%}$

Таким образом, занижение оценки *PFDavg* по формуле (1) по сравнению с оценкой по формуле (2) равно $3{,}98\cdot10^{-7}$, что составляет 26,7% от значения $1{,}49\cdot10^{-6}$. Можно показать, что при уменьшении показателя *DC* занижение оценки $PFDavg_{1oo1}$ становится незначительным. Так, выполнив расчет для полугодового интервала между контрольными проверками при *DC* = 90%, получим значение *PFDavg* по формуле (1), равное $1{,}095\cdot10^{-5}$, значение *PFDavg* по формуле (2), равное $1{,}133\cdot10^{-5}$. Занижение оценки $PFDavg_{1oo1}$ составляет $3{,}8\cdot10^{-7}$ или 3,4% от значения, рассчитанного по формуле (2).

Метод анализа деревьев неисправностей

Рассмотрим архитектуру дублированного канала 1oo2, состоящего из идентичных элементов с интенсивностями опасных обнаруженных отказов λ_{du}. Структура 1oo2 означает, что функция безопасности будет выполнена, если функционирует хотя бы один элемент. Тогда вероятность безотказной работы дублированного канала в предположении экспоненциального распределения наработки до отказа рассчитывается по формуле

$$R_{1oo2}(t) = 2e^{-\lambda_{du}t} - e^{-2\lambda_{du}t}.$$

Средняя вероятность отказа на межконтрольном интервале [2]

$$PFD_{avg\,1oo2} = 1 - \frac{1}{TI}\int_0^{TI} R_{1oo2}(t)\,dt =$$

$$= 1 - \frac{1}{TI}\int_0^{TI}\left(2e^{-\lambda_{du}t} - e^{-2\lambda_{du}t}\right)dt =$$

$$= 1 - \frac{2}{\lambda_{du}TI}(1 - e^{-\lambda_{du}TI}) + \frac{1}{2\lambda_{du}TI}(1 - e^{-2\lambda_{du}TI}). \qquad (3)$$

Выражение (3) может быть упрощено при использовании первых двух членов разложения в ряд Тейлора в предположении $\lambda_{du}TI \ll 1$:

$$PFD_{avg\,1oo2} \approx \frac{(\lambda_{du}TI)^2}{3}. \qquad (4)$$

Выражение для расчета вероятности отказа, которое получается при использовании метода ДН, если в качестве исходных данных для каждого элемента использовать формулу (1), имеет вид

$$PFD_{avg\,1oo2\,ДН} \approx \frac{(\lambda_{du}TI)^2}{4}. \qquad (5)$$

Заниженное значение средней неготовности объясняется именно тем фактом, что произведение средних не является средним произведения.

Таким образом, для получения корректного консервативного значения средней неготовности дублированного канала, рассчитанного по формуле (4), значение, полученное при структурном моделировании ДН (5), следует умножить на корректирующий коэффициент, равный 4/3.

Рассмотрим для примера широко используемую в современных системах ПАЗ структуру 2oo3. Пусть все элементы равнонадежны и имеют одинаковую интенсивность опасных необнаруженных отказов λ_{du}. Структура 2oo3 означает, что функция безопасности будет выполнена, если функционирует как минимум 2 элемента.

Вероятность безотказной работы голосующей структуры 2oo3 в предположении экспоненциального распределения наработки до отказа рассчитывается по формуле

$$R_{2oo3}(t) = 3e^{-2\lambda_{du}t} - 2e^{-3\lambda_{du}t}. \qquad (6)$$

Средняя неготовность на межконтрольном интервале есть [2]

$$PFD_{avg\,2oo3}\Big| = 1 - \frac{1}{TI}\int_0^{TI} R_{2oo3}(t)\,dt =$$

$$= 1 - \frac{1}{TI}\int_0^{TI}\left(3e^{-2\lambda_{du}t} - 2e^{-3\lambda_{du}t}\right)dt =$$

$$= 1 - \frac{3}{2\lambda_{du}TI}\left(1 - e^{-2\lambda_{du}TI}\right) + \frac{2}{3\lambda_{du}TI}\left(1 - e^{-3\lambda_{du}TI}\right). \qquad (7)$$

Выражение (7) может быть упрощено при использовании первых двух членов разложения в ряд Тейлора в предположении $\lambda_{du}TI \ll 1$. Тогда

$$PFD_{avg\,2oo3} \approx (\lambda_{du}TI)^2. \qquad (8)$$

Консервативная оценка вероятности отказа структуры 2oo3 при $\lambda_{du}TI \ll 1$ при использовании ДН может быть записана в виде

$$PFD_{avg\,2oo3\,ДН} \approx 3PFD_{1oo2} =$$

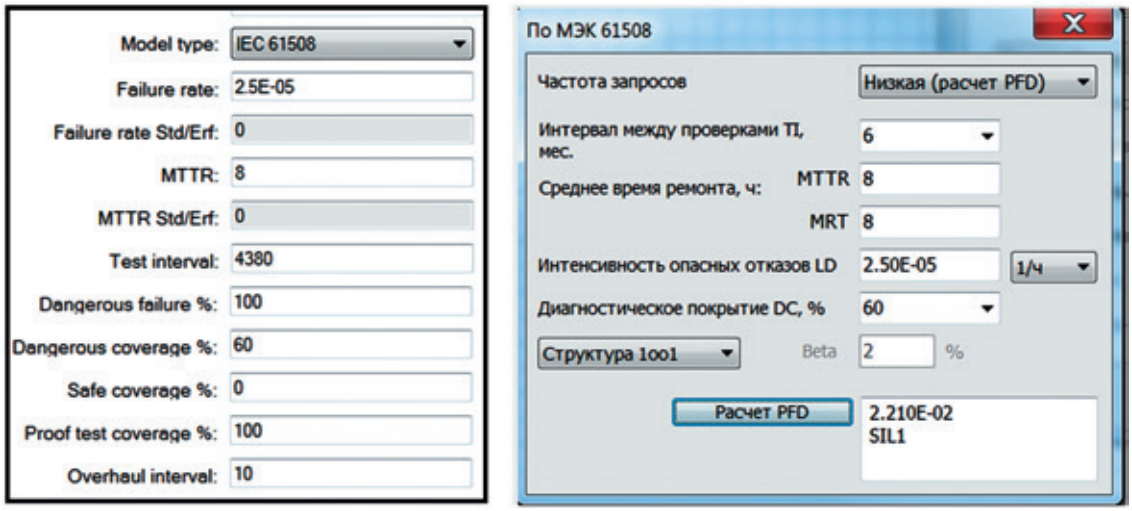
$$= 3\cdot\left(\frac{\lambda_{du}TI}{2}\right)^2 = \frac{3}{4}(\lambda_{du}TI)^2. \qquad (9)$$

С учетом выражения (5) для получения корректного консервативного значения средней неготовности структуры 2oo3 при моделировании ДН необходимо ввести в формулу (9) корректирующий коэффициент, равный 4/3.

Рассмотрим общий случай неидентичных по надежности каналов. Пусть имеется голосующая группа *KooN*, для которой условием функционирования является отсутствие опасных необнаруженных отказов в *K* из *N* каналах, а условием отказа является отказ *N*–*K*+1 каналов. Можно показать, что для получения консервативной оценки средней неготовности избыточной структуры при использовании ДН следует использовать корректирующие коэффициенты вида [2]

$$K_{PFD\,ДН} = \frac{2^{N-K+1}}{N-K+2}. \qquad (12)$$

Корректирующие коэффициенты для некоторых структур *K* из *N* представлены в табл. 2.



а) б)

Рис. 1. Экранные интерфейсы программ Isograph Reliability Workbench (а) и ПК АРБИТР (б)

Таблица 2 – Корректирующие коэффициенты для метода ДН

$N-K+1$	$K_{PFD\ ДН}$
2	4/3 ≈ 1,33
3	2,00
4	16/5 ≈ 3,20

В современных программных пакетах в качестве исходных данных для моделирования ДН показатели функциональной безопасности $PFD_{avg\ 1oo1}$ рассчитываются по формулам стандарта [1] с помощью встроенных калькуляторов.

На рис. 1 показаны экранные интерфейсы программных пакетов ПК АРБИТР [4] и Isograph Reliability Workbench [5] с инструментами для ввода исходных данных в формате стандарта МЭК 61508.

Учет отказов по общей причине

Современные методы анализа надежности сложных технических систем, обладающих избыточностью, предполагают учет отказов по общей причине [6].

Стандарты серии МЭК 61508 «Функциональная безопасность» рекомендуют использовать при оценке надежности систем ПАЗ бета-модель ООП (модель β-фактора).

Обозначим суммарную (общую) вероятность отказа каждого элемента, входящего в группу ООП, обусловленную как независимыми отказами, так и отказами по общей причине, через q_i^{tot}. Предположим, что элементы могут отказать как по независимой причине с вероятностью $q_i^{нез}$, так и по общей причине – с некоторой вероятностью $q_i^{ООП}$. В этом случае

$$q_i^{tot} = q_i^{нез} + q_i^{ООП}. \quad (13)$$

При построении ДН исходные данные базисных событий задаются в виде q_i^{tot}, а величины $q_i^{нез}$ и $q_i^{ООП}$ вычисляются по формулам

$$q_i^{нез} = (1-\beta) q_i^{tot}, \quad (14)$$

$$q_i^{оол} = \beta q_i^{tot}. \quad (15)$$

Рассмотрим для примера дублированную систему с параметрами [9]:

$$\beta=1/4,\ q_1 = q_2 = 3/4.$$

Рассчитаем составляющие вероятности отказа системы согласно (14) и (15) при условии, что статистика по отказам элементов включают в себя независимую составляющую и составляющую ООП, то есть $q_1 = q_2 = q_{tot}$.

$$q_1^{нез} = q_2^{нез} = (1-1/4)\cdot\frac{3}{4} = 0,5625.$$

$$q_{1,2}^{ООП} = \frac{1}{4}\cdot\frac{3}{4} = \frac{3}{16} = 0,1875.$$

При построении ДН логическая функция такой системы будет иметь вид

$$s = x_1 x_2 \vee ООП(x_1, x_2). \quad (16)$$

В ортогональной форме логическая функция (16) будет иметь вид

$$s = x_1 x_2 \overline{ООП(x_1, x_2)} \vee ООП(x_1, x_2). \quad (17)$$

Вероятностная функция для вычисления вероятности отказа дублированной структуры Qs, соответствующая (16), будет иметь вид

$$Q_{s\,ООП} = q_1^{нез} q_2^{нез} \left(1 - q^{ООП}\right) + q^{ООП} =$$
$$= 0,5625 \cdot 0,5625 \cdot (1 - 0,1875) + 0.1875 =$$
$$= 0,444458. \quad (18)$$

Без учета ООП вероятность отказа дублированной системы рассчитывается с учетом независимой составляющей вероятности отказа элементов, то есть

$$Q_s = q_1^{нез} q_2^{нез} = 0,5625 \cdot 0,5625 = 0,31640625. \quad (19)$$

Сравнение (18) и (19) показывает, что в соответствии с определением и моделью (13) отказы по общей причине являются дополнительными факторами, снижающими надежность резервированных систем. Поэтому следует считать вывод о повышении надежности при учете ООП [6] физически неправильным и математически некорректным.

Выражения (13), (14) и (15) применяют, в основном, тогда, когда вероятности отказов элементов ПАЗ оцениваются по статистическим, эксплуатационным данным конечных пользователей. При этом предполагается, что статистика общего потока отказов включает в себя как независимые (собственные) отказы изделий, так и отказы, вызванные общими причинами.

При проектном расчете надежности ПАЗ, когда используются справочные данные о надежности компонентов, возможно введение коррекции на «будущие» эксплуатационные ООП. В этом случае общая вероятность отказа рассчитывается по формуле

$$q_i^{tot} = q_i^{np} + q_i^{np}\beta, \qquad (20)$$

где $q_i^{\text{пр}}$ – проектная оценка вероятности отказа i-го элемента ПАЗ, полученная на основе справочных данных о надежности резисторов, конденсаторов, микросхем и т.д.).

Тогда выражение (18) будет иметь вид

$$Q_{s\,OOП} = q_1^{np} q_2^{np}\left(1 - q^{OOП}\right) + q^{OOП} =$$
$$= 0,75 \cdot 0,75 \cdot (1 - 0,1875) + 0,1875 = 0,64453. \qquad (21)$$

Результат (21) является консервативным, что приемлемо при решении задач функциональной безопасности. Определение количественных значений параметра β весьма важно, так как зачастую вклад ООП существенно влияет на оценку *PFDavg*, от которой зависит назначение или подтверждение уровня полноты безопасности контура ПАЗ. Для иллюстрации влияния количественных значений параметра β на оценку *PFDavg* рассмотрим несколько примеров из стандарта МЭК 61508-6. В стандарте приведены таблицы с расчетами показателя *PFDavg* для архитектур 1oo2, 1oo3 и 2oo3.

Для указанных архитектур возможно применение приближенных формул в виде

$$PFD_{avg\,1oo2} \approx \frac{4}{3}(PFD_{1oo1})^2 + \beta \cdot PFD_{1oo1}, \qquad (22)$$

$$PFD_{avg\,1oo3} \approx 2 \cdot (PFD_{1oo1})^3 + \beta \cdot PFD_{1oo1}, \qquad (23)$$

$$PFD_{avg\,2oo3} \approx 4 \cdot (PFD_{1oo1})^2 + \beta \cdot PFD_{1oo1}. \qquad (24)$$

Структура формул (22)–(24) позволяет показать распределение долей вероятности отказа, которые определяются значениями интенсивности опасных необнаруженных отказов λ_{du} – структурная составляющая (первое слагаемое в формулах) и отказов по общим причинам (второе слагаемое в формулах). Например, при $PFDavg_{\ 1oo1} = 6,25 \cdot 10^{-3}$, β = 2 и 10% распределение причин отказа для архитектуры 1oo2 будет следующим:

β=2%:

$$PFD_{avg\,1oo2} = \underbrace{\frac{4}{3}(6,25e^{-3})^2}_{29,4\%} + \underbrace{0,02 \cdot 6,25\text{e}^{-3}}_{70,6\%} = 1,77\text{e}^{-4};$$

β=10%:

$$PFD_{avg\,1oo2} \approx \underbrace{\frac{4}{3}(6,25e^{-3})^2}_{7,7\%} + \underbrace{0,1 \cdot 6,25e^{-3}}_{92,3\%} = 6,77e^{-4}.$$

Естественно, что при увеличении значения параметра β определяющим является второе слагаемое в формулах, относящееся к ООП. В этом случае занижение оценки средней неготовности относительно формул стандарта [1] за счет «структурной составляющей» становится незначительным.

На рис. 2 показаны графики изменения относительных величин занижения *PFDavg* в зависимости от коэффициента β для структур 1oo2 и 2oo3 при трех значениях интенсивности опасных необнаруженных отказов λ_{du} ($2,5 \cdot 10^{-5}$, $2,5 \cdot 10^{-6}$ и $2,5 \cdot 10^{-7}$ 1/ч). Значения *PFDavg* получены с использованием метода ДН и с коррекцией по формуле (20).

Анализ графиков показывает, что при увеличении значений коэффициента β относительное занижение

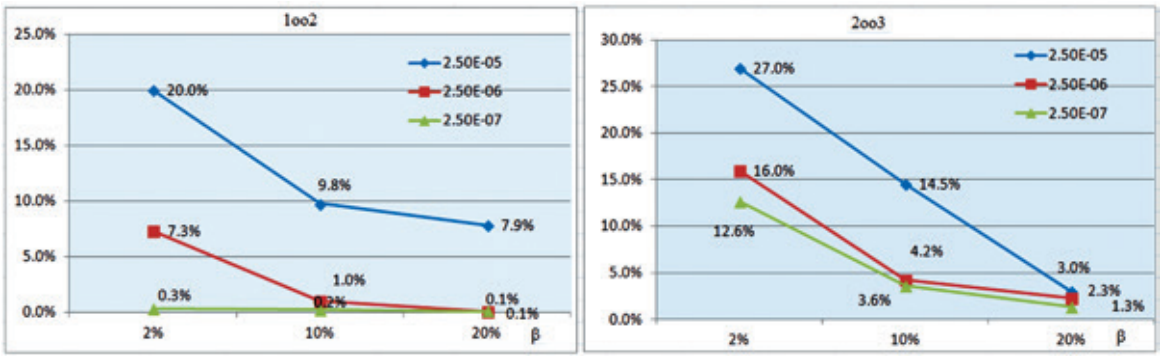


Рис. 2. Относительное занижение оценки *PFDavg* при расчетах с использованием метода деревьев отказов

оценки *PFDavg* уменьшается. Кроме того, следует заметить, что относительное занижение особенно проявляется при моделировании ДН менее надежных избыточных структур, показатели которых соответствуют границе диапазона уровня полноты безопасности УПБ1.

На рис. 3 представлены графики зависимости оценок *PFDavg* для структуры 2oo3 при различных исходных данных в виде значений PFD_{1oo1} для структуры 1oo1. Параметр модели ООП β = 2%.

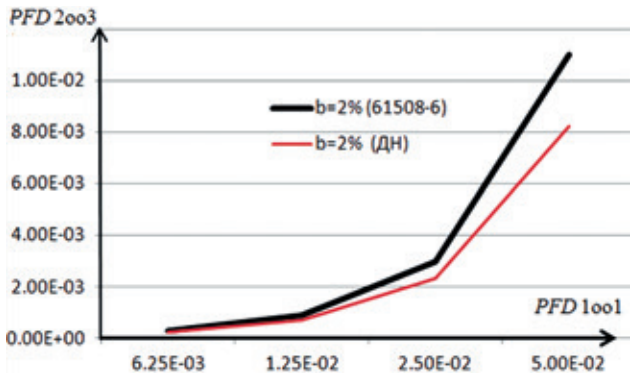


Рис. 3. Оценки параметра *PFDavg* для структуры 2oo3

На рис. 3 темная кривая отражает результаты использования формулы (24), которая практически совпадает с формулами стандарта МЭК 61508-6. Светлая кривая отражает результаты моделирования надежности ПАЗ с использованием метода ДН. При значениях PFD_{1oo1} меньше $1{,}25 \cdot 10^{-2}$ (граница интервала для УПБ1) занижение оценки вероятности отказа на запрос для структуры 2oo3 становится незначительным. При более высоких значениях вероятности отказа на запрос элемента ПАЗ оценки надежности структуры разными методами могут привести к совершенно разным результатам. Так при $PFDavg_{1oo1} = 5{,}5 \cdot 10^{-2}$ результат расчета по формуле (24), а также данные таблиц стандарта МЭК 61508-6, позволяет сделать вывод о соответствии контура ПАЗ УПБ1. Расчеты методом ДН приводят к выводам о соответствии контура УПБ2. Здесь можно сделать вывод, что при моделировании надежности ПАЗ методом ДН, необходимо анализировать как исходные данные о надежности компонентов, так и полученные результаты.

При низкой надежности компонентов, соответствующей верхней границе УПБ1, разумно применять поправочные коэффициенты (12) для получения гарантированной консервативной оценки надежности системы ПАЗ.

Как подчеркивает стандарт МЭК 61508-6, коррекция результатов применения классических логических методов, например, ДН, с теоретической точки зрения не так проста. Поэтому при расчете надежности систем следует глубоко анализировать возможности достижения высокого системного УПБ при относительно низкой надежности компонентов и учете ООП.

Заключение

Таким образом, в настоящей статье проведен анализ возможных ошибок при определении уровня полноты безопасности контура системы ПАЗ, которые могут возникать при использовании метода ДН в коммерческих программных пакетах. Причинами таких ошибок являются, во-первых, завышение надежности компонентов контура ПАЗ за счет применения упрощенной формулы для расчета средней неготовности нерезервированного элемента без учета опасных обнаруженных отказов. Для устранения этой причины следует использовать точные формулы стандарта МЭК 61508-6. Второй причиной является расчет средней неготовности контура с избыточной структурой по средней неготовности его компонентов. Для устранения данной причины следует либо использовать корректирующие коэффициенты, либо рассчитывать именно среднее значение неготовности контура на заданном межконтрольном интервале.

Библиографический список

1. ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. 2012. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р 61508-3. М.: Стандартинформ, 2014. 110 с.

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

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

4. Можаев А.С. Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб. М.: РНЦ «Курчатовский институт», 2008. Вып. 2/2008. С. 105–116.

5. Reliability Workbench – Isograph [Электронный ресурс]. URL: https://www.isograph.com/software/reliability-workbench/ (Дата обращения 03.08.2022).

6. Антонов А.В., Чепурко В.А., Черняев А.Н. Исследование модели учета отказов по общей причине бета-фактора // Надежность. 2019. №2. С. 9–17. DOI: 10.21683/1729-2646-2019-19-2-9-17

7. Можаева И.А., Струков А.В. Применение ПК АРБИТР для проектной оценки показателей функциональной безопасности систем противоаварийной защиты // В сборнике: Труды 4-й Международной научно-практической конференции «Имитационное и комплексное моделирование морской техники и морских транспортных систем» (ИКМ МТМТС – 2017). С-Петербург, 2017. С. 100–105.

References

1. GOST R IEC 61508. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Moscow: Standartinform; 2014. (in Russ.)

2. Rausand M. Reliability of Safety-Critical Systems: Theory and Applications. Willey; 2014.

3. Mozhaeva I.A., Nozik A.A., Strukov A.V. [Generic examples of functional safety calculation of emergency shutdown systems of hazardous industrial facilities]. In: [Proceedings of the Twentieth All-Russian Research and Practice Conference Topical Problems of Safety and Security, Vol. 2, Counter-Terrorist Measures]. Moscow: RARAN; Saint Petersburg: NPO SM; 2019. Pp. 486-494. (in Russ.)

4. Mozhaev A.S. Annotation for the ARBITR software (PK ASM SZMA). In: [Matters of Nuclear Science and Engineering. Nuclear Reactor Physics Series. Annotations for Rostekhnadzor-Certified Software. A Collection of Research and Engineering Papers]. Moscow: Kurchatov Institute 2008;2:105-116. (in Russ.)

5. https://www.isograph.com/software/reliability-workbench/ (accessed 03.08.2022).

6. Antonov A.V., Chepurko V.A., Cherniaev A.N. Research of the beta-factor model of accounting for common cause failures. *Dependability* 2019;2:9-17. DOI: 10.21683/1729-2646-2019-19-2-9-17.

7. Mozhaeva I.A., Strukov A.V. [Application of PK ARBITR for engineering assessment of functional safety indicators of emergency shutdown systems]. In: [Proceedings of the 4-th International Research and Practice Conference Simulation of Marine Facilities and Marine Transportation Systems (IKT MTMTS 2017)]. Saint Petersburg; 2017. Pp. 100-105. (in Russ.)

Сведения об авторах

Можаева Ирина Александровна – кандидат технических наук, ведущий специалист исследовательского отдела ООО «СПИК СЗМА», 26-я линия В.О., д. 15, корп. 2, лит. А, Бизнес-центр «Биржа», Санкт-Петербург, Российская Федерация, 199106, e-mail: irina_mozhaeva@szma.com

Струков Александр Владимирович – кандидат технических наук, доцент, ведущий специалист исследовательского отдела ООО «СПИК СЗМА», 26-я линия В.О., д. 15, корп. 2, лит. А, Бизнес-центр «Биржа», Санкт-Петербург, Российская Федерация, 199106, e-mail: alexander_strukov@szma.com

About the authors

Irina A. Mozhaeva, Candidate of Engineering, Lead Specialist of the Research Unit, SPIK SZMA 15, korp. 2, lit. A 26-ya Liniya Vasiliyevskogo Ostrova, Birzha Business Centre, 199106, mailto:irina_mozhaeva@szma.comSaint Petersburg, Russian Federation, e-mail: irina_mozhaeva@szma.com

Alexander V. Strukov, Candidate of Engineering, Associate Professor, Lead Specialist of the Research Unit, SPIK SZMA 15, korp. 2, lit. A 26-ya Liniya Vasiliyevskogo Ostrova, Birzha Business Centre, 199106, mailto:alexander_strukov@szma.comSaint Petersburg, Russian Federation, e-mail: alexander_strukov@szma.com

Вклад авторов в статью

Можаева И.А. – разработка программы для подготовки и ввода исходных данных в формате требований стандарта ГОСТ Р МЭК 61508, анализ погрешностей при решении задач функциональной безопасности в программной среде ПК АРБИТР.

Струков А.В. – анализ приближенных и упрощенных формул оценки показателей функциональной безопасности для типовых архитектур систем ПАЗ.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.