

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

И. А. Можаяева, А. В. Струков (Санкт-Петербург)

Введение

Проектная оценка показателей функциональной безопасности систем противоаварийной защиты (ПАЗ), использующих электрические/электронные/программируемые электронные технологии, согласно, например, рекомендациям нормативных документов Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) при проведении анализа опасностей, связанных с отказами технических устройств, осуществляется с использованием соответствующих методов теории надежности.

Определение показателей надежности и безопасности для современных технических средств представляет собой сложную комплексную задачу системного анализа, выполнение которой даже при наличии разработанного методического обеспечения невозможно или крайне затруднено без использования соответствующих программных средств. К таким программным средствам относится отечественный программный комплекс (ПК) «АРБИТР» [1], разработанный в АО «Специализированная инжиниринговая компания «Севзапмонтажавтоматика» (АО «СПИК СЗМА») и аттестованный Ростехнадзором. Реализованный в ПК АРБИТР автоматизированный структурно-логический метод моделирования надежности, безопасности и технического риска дает возможность оперативной адаптации алгоритмов и процедур для решения современных задач системного анализа, в том числе, и анализа функциональной безопасности.

1. Нормативные требования в области функциональной безопасности

Общие подходы к вопросам обеспечения безопасности на всех стадиях жизненного цикла ПАЗ подробно изложены в серии стандартов ГОСТ Р МЭК 61508 и ГОСТ Р МЭК 61511. Стандарты устанавливают необходимость проведения анализа опасностей и риска ПАЗ, применяемых в промышленных процессах и разработанных в соответствии с требованиями МЭК 61508. Указанные стандарты в целях реализации рациональной и последовательной технической политики устанавливают подход, минимизирующий стандартизацию для всех этапов жизненного цикла безопасности. Концепция жизненного цикла безопасности предполагает, что для каждой стадии этого процесса должны быть определены входы, выходы, а также действия по верификации правильности их определения.

Для этапа разработки и проектирования основной задачей (выходом) является проектирование систем ПАЗ, отвечающих требованиям к функциям безопасности и соответствующих заданному уровню полноты безопасности (УПБ). Под полнотой безопасности понимается средняя вероятность того, что ПАЗ удовлетворительно выполняет требуемые функции безопасности при всех заданных условиях и в течение заданного периода времени.

Уровень полноты безопасности – УПБ (safety integrity level; SIL) – это дискретный уровень, принимающий одно из четырех возможных значений, определяющий требования к полноте безопасности для функций безопасности ПАЗ. Уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности, уровень, равный 1, отвечает наименьшей полноте безопасности.

Входными данными для этапа разработки и проектирования ПАЗ являются требования по безопасности и УПБ, установленные в спецификации на основе распределения требований к безопасности. Эти входные требования являются выходами начальной стадии жизненного цикла безопасности – анализа опасностей и риска (рис.1).

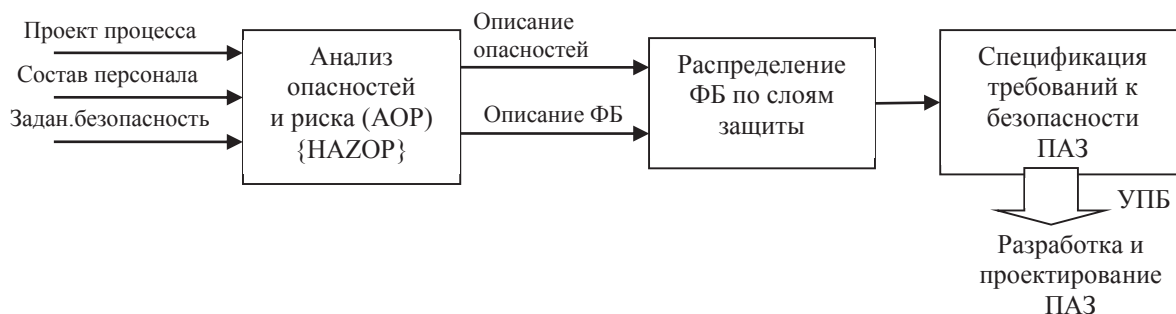


Рис. 1. Фрагмент жизненного цикла безопасности

Первым шагом в оценке УПБ является определение минимально необходимых требований к архитектуре канала ПАЗ, определяемых требованиями к аппаратной отказоустойчивости. Аппаратная отказоустойчивость характеризует способность компонента (элемента, подсистемы) выполнять заданную функцию безопасности при наличии одного или более опасного отказа. Требования отказоустойчивости аппаратных средств формируются с минимальной избыточностью. В дальнейшем в зависимости от интенсивности запросов на обслуживание интервала между контрольными проверками для обеспечения заданного значения УПБ может возникнуть необходимость в дополнительной избыточности. В таблице 1 представлено минимально допустимое число отказов устройств для различных уровней полноты безопасности.

Таблица 1

Минимально допустимое число отказов

УПБ	Минимально допустимое число отказов		
	SFF (ДБО) < 60%	60% ≤ SFF (ДБО) ≤ 90%	SFF (ДБО) > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Специальные требования		

Из таблицы 1 видно, что минимальные требования к архитектуре канала ПАЗ главным образом определяются долей безопасных отказов (ДБО, SFF в английской аббревиатуре). При этом следует помнить, что методика расчета показателей безопасности ПАЗ, представленная в ГОСТ Р МЭК 61508-6, предполагает, что элемент ПАЗ имеет интенсивность опасных отказов менее 10^{-5} (1/час).

В качестве примеров архитектуры с отказоустойчивостью, равной 0, можно привести архитектуры 1oo1, 2oo2, 3oo3, с отказоустойчивостью 1 – архитектуры 1oo2, 1oo2D, 2oo3, с отказоустойчивостью 2 – архитектуру 1oo3.

Одним из разделов спецификации требований при проектировании системы ПАЗ являются требования к значению вероятности отказа при наличии запроса на выполнение функции безопасности. Эти требования должны быть проверены расчетом, при

этом значение вероятности отказа должно быть не более целевой меры отказов, установленной в спецификациях требований к безопасности.

Для функций безопасности ПАЗ, выполняемых в режиме по запросу, целевая мера отказов выражается в терминах средней вероятности отказа ($PFDAvg$) выполнения по запросу предусмотренной функции безопасности для режима низкой интенсивности запросов или в терминах средней частоты опасных отказов (PFH) для режима с высокой интенсивностью запросов или режима с непрерывным запросом (табл. 2).

Таблица 2

Уровни полноты безопасности

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	$\geq 10^{-2} PFD < 10^{-1}$	$\geq 10^{-6} PFH < 10^{-5}$

Количественная оценка вероятности отказа $PFDAvg$ выполняется для каждой функции безопасности ПАЗ, так как им могут быть свойственны различные виды отказов компонентов и архитектур ПАЗ в части резервирования.

2. Методологическая и алгоритмическая основы оценки вероятности отказа на запрос

По физическому смыслу $PFDAvg$ есть средняя неготовность системы на интервале между контрольными проверками. Расчет $PFDAvg$ основан на учете двух типов неготовности канала:

1 – неизвестная, когда простой ПАЗ 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.

Алгоритмическая основа методики оценки $PFDAvg$ различных архитектур – приближенные формулы стандарта IEC 61508-6 для расчета $PFDAvg$ простых типовых архитектур 1oo1 и 1oo2D.

Основная идея IEC 61508-6 состоит в расчете $PFDAvg$ канала, представленного как один элемент, характеризуемый средней групповой частотой опасных отказов λ_{DG} и эквивалентным групповым временем простоя t_{GE} [3].

$$PFDAvg^{(G)} = F(\lambda_{DG}, t_{GE}, MTTR, MRT) \quad (1)$$

Так как состояние системы безопасности полностью определяется состоянием ее элементов, то системный показатель функциональной безопасности рассчитывается с использованием структурной функции системы, то есть

$$PFDAvg_{sys} = P\{PFDAvg_1, \dots, PFDAvg_i, \dots, PFDAvg_n\} \quad (2)$$

$$PFH_{sys} = P\{PFH_1, \dots, PFH_i, \dots, PFH_n\} \quad (3)$$

где $PFDAvg_{sys}$, PFH_{sys} – системные показатели функциональной безопасности;

PFD_i , PFH_i – показатели функциональной безопасности i -го компонента;
 $P\{\dots\}$ – структурная функция системы.

3. Методика расчета средней вероятности отказа на запрос

В общем виде методика расчета PFD_{avg} канала включает в себя следующие шаги:

I. формирование исходных данных, необходимых для расчета вероятностей отказа на запрос для всех элементов системы;

II. расчет с помощью утилиты вероятностей отказа на запрос структур с архитектурой 1001 и 1002D по формулам стандарта ГОСТ Р МЭК 51508-6;

III. построение схемы функциональной целостности (СФЦ) в виде структурной схемы надежности или дерева неисправностей системы безопасности и моделирование надежности системы безопасности с учетом особенностей построения голосующих групп в программной среде ПК АРБИТР [2].

Формирование исходных данных, необходимых для расчета показателей функциональной безопасности, осуществляется на основе анализа документации производителей компонентов.

Для расчета показателей функциональной безопасности архитектур 1001 и 1002D в программной среде ПК АРБИТР разработана утилита «Расчет вероятности отказа на запрос PFD_{avg} ». Экранный интерфейс утилиты представлен на рис.2.

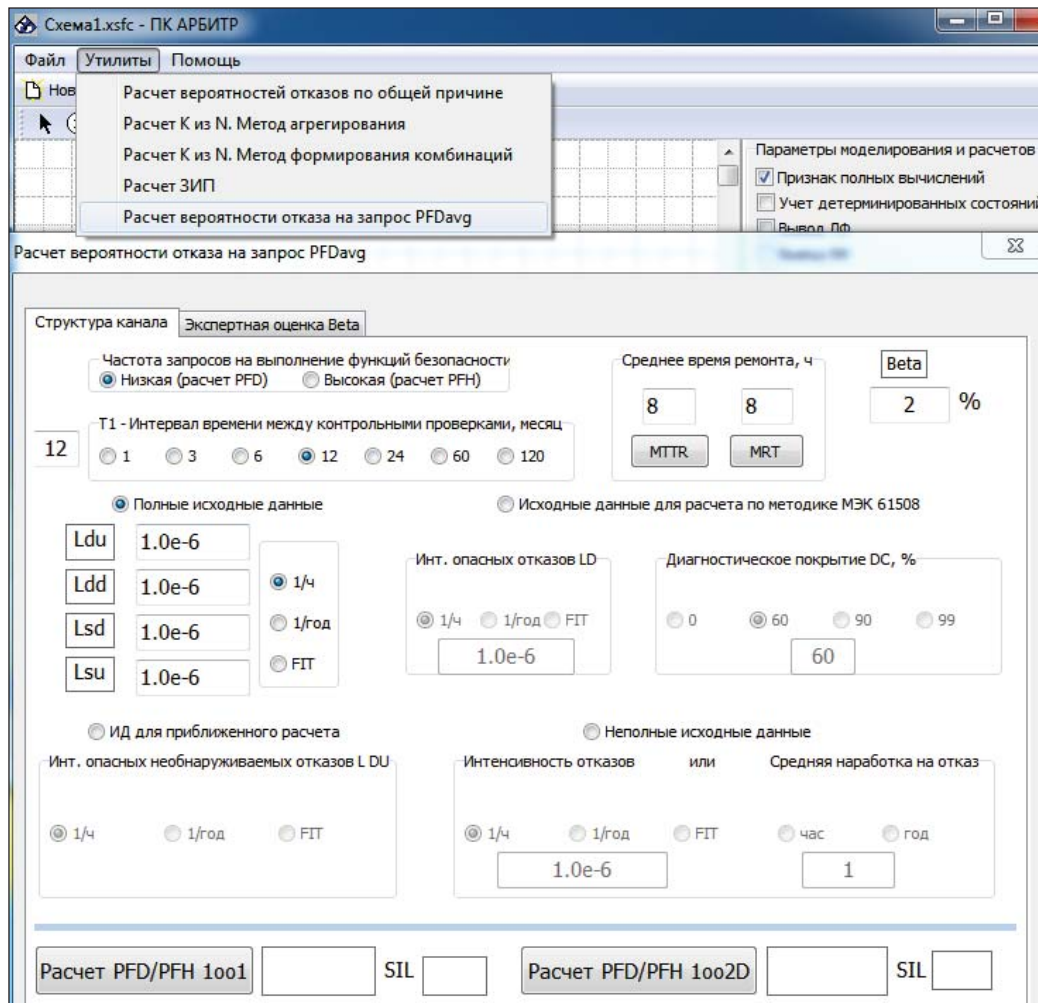


Рис. 2. Утилита «Расчет вероятности отказа на запрос PFD_{avg} »

Для ввода исходных данных и расчета показателей на странице «Структура канала» выбираются следующие режимы и вводятся исходные данные:

– частота запросов на выполнение функций безопасности: низкая (расчет PFH), если частота запросов не выше 1 раза в год, высокая (расчет PFH) – если частота запросов выше 1 раза в год;

– интервал времени между контрольными проверками (в тексте стандартов серии МЭК 61508 обозначен через T_I , в месяцах). Для высокой частоты запросов интервал T_I обычно выбирается из дискретного ряда 1, 3, 6, 12 месяцев, для низкой частоты запросов – из ряда 6, 12, 24 и 120 месяцев. По умолчанию задается 12 месяцев;

– среднее время восстановления (MTTR) и средняя продолжительность ремонта (MRT). Обычно по умолчанию задается $MTTR = MRT = 8$ ч.

Исходные данные об интенсивностях отказов для отдельных компонентов систем ПАЗ обычно приводятся производителями компонент в «Руководстве по функциональной безопасности». Учитывая, что разные производители и вендеры по-разному формируют данные по надежности и безопасности, в утилите предусмотрены четыре режима ввода исходных данных об интенсивностях отказов компонент.

Полные исходные данные включают в себя следующие данные об интенсивностях отказов:

- опасных необнаруженных – Ldu ;
- опасных обнаруженных – Ldd ;
- безопасных необнаруженных – Lsu ;
- безопасных обнаруженных – Lsd .

Значения интенсивностей отказов могут иметь размерности «1/час», «1/год» или FIT (10^{-9} 1/час).

Исходные данные для расчета по методике МЭК 61508 включают в себя:

- данные об интенсивностях опасных отказов Ld ;
- значение диагностического охвата, в %.

Значения интенсивности опасных отказов также могут иметь размерности «1/час», «1/год» или FIT.

Исходные данные для приближенного расчета включают в себя данные об интенсивностях опасных необнаруженных отказов Ldu .

В этом случае для структуры 1001 $PFH_{1001} \approx \frac{Ldu T_I}{2}$, для структуры 1002D $PFH_{1002D} \approx \left(\frac{Ldu T_I}{2}\right)^2$, при учете отказов по общей причине $PFH_{1002D} \approx \frac{\beta Ldu T_I}{2}$, где β – параметр бета-модели отказов по общим причинам (ООП).

Неполные исходные данные предполагают использование следующих допущений:

• при задании интенсивности отказов $Ldu = Ldd = Lsu = Lsd = L/4$, где L – общая (суммарная) интенсивность отказов.

Значения интенсивности отказов могут иметь размерности «1/час», «1/год» или FIT;

• при задании средней наработки на отказ T_0 общая (суммарная) интенсивность отказов $L = 1/T_0$.

Пересчет размерности производится с условием 1 год = 8760 час.

Формирование исходных данных на структурном уровне состоит в оценке показателей безопасности каналов с архитектурами 1001 и 1002D по формулам, приведенным в стандарте ГОСТ Р МЭК 61508-6.

Заключение

Графические и вычислительные средства ПК АРБИТР представляют собой мощный и удобный в инженерном смысле слова инструмент для автоматизированного анализа моделирования надежности и функциональной безопасности систем ПАЗ. Для подготовки исходных данных для элементов ПАЗ используется встроенная утилита, позволяющая рассчитать показатели PFD_{avg} канала для базовых структур 1oo1 и 1oo2D. Моделирование системных показателей осуществляется на основе методологии автоматизированного структурно-логического моделирования.

Литература

1. **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.
2. **Можаева И. А., Нозик А. А., Струков А. В.** Программная реализация методов количественного анализа риска аварий опасных производственных объектов на основе логико-вероятностного и логико-детерминированного подходов // Наука и безопасность. 2016. №2/20. С.26–36.
3. **Rausand M.** Reliability of Safety-Critical Systems: Theory and Applications. Willey. 2014. 448 p.