ПРОГРАММНЫЙ КОМПЛЕКС «АРБИТР» – ИНСТРУМЕНТ ДЛЯ ПРОЕКТНОЙ ОЦЕНКИ НАДЕЖНОСТИ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ

М.С. СКВОРЦОВ (АО “СПИК СЗМА”)

Одним из основных требований, учитываемых при создании систем управления опасными производственными объектами, является реализация проектных решений с учетом показателей надежности и функциональной безопасности. В статье рассмотрены существующие на данный момент нормативно-технические документы, регламентирующие требования к надежности автоматизированных систем управления. Показана возможность использования отечественного программного комплекса “АРБИТР” для выполнения проектной оценки надежности систем управления и обоснования функциональной безопасности систем противоаварийной автоматической защиты.

Ключевые слова: *надежность, функциональная безопасность, ПК “АРБИТР”, уровень полноты безопасности, проектная оценка надежности, обоснование функциональной безопасности.*

ВВЕДЕНИЕ

Одним из основных требований, учитываемых при создании систем управления опасными производственными объектами (ОПО), является реализация проектных решений с учетом показателей надежности и безопасности.

В связи с этим в середине 60-х годов прошлого века были начаты (и продолжаются в настоящее время) работы по развитию теории, методов анализа и расчета надежности. Именно в эти годы профессор Рябинин И.А. разработал логико-вероятностный метод моделирования и расчета надежности [1-3], который первоначально использовался для моделирования и расчета надежности корабельных энергетических систем. Работу в этом направлении продолжил профессор Можаев А.С., который разработал общий логико-вероятностный метод моделирования и расчета надежности структурно-сложных технических систем [4], а также простой и в тоже время универсальный графический аппарат схем функциональной целостности [5] для описания структуры и взаимодействия элементов системы. Под руководством профессора Можаева А.С. в АО “СПИК СЗМА” были выполнены теоретические и программные разработки, которые стали основой для решения инженерных задач, связанных с проектной оценкой надежности и безопасности систем управления.

Определение показателей надежности и безопасности для современных комплексов технических средств автоматизации 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”, разработанный АО “СПИК СЗМА” и аттестованный Ростехнадзором [6]. Используемые в ПК “АРБИТР” общий логико-вероятностный метод и технология автоматизированного структурно-логического моделирования позволяют решать задачи моделирования и расчета надежности [7] безопасности и риска [8]. Прохождение ПК “АРБИТР” процедуры верификации результатов моделирования и расчетов в специализированном экспертном комитете Ростехнадзора позволяет гарантировать адекватность применяемых методов моделирования, а также правильность и достоверность расчетов. ПК “АРБИТР” зарегистрирован в реестре российского программного обеспечения Минкомсвязи.

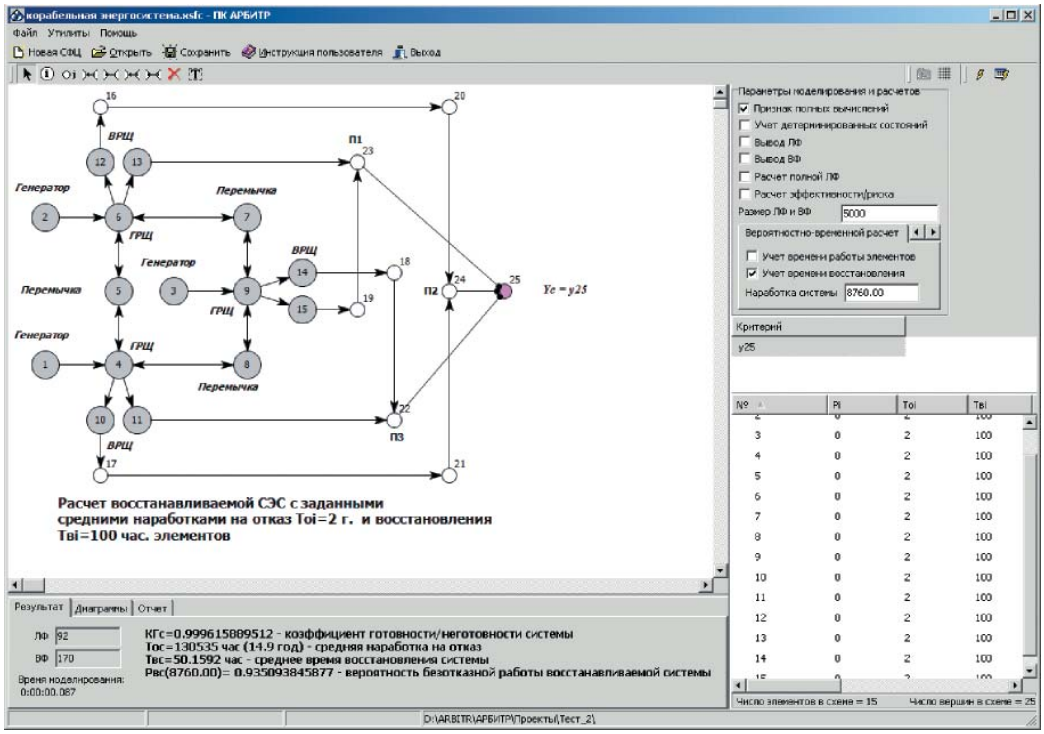

Рис. 1. Интерфейс программного комплекса "АРБИТР"

ПРОЕКТНАЯ ОЦЕНКА НАДЕЖНОСТИ СИСТЕМ УПРАВЛЕНИЯ

Использование ПК "АРБИТР" для проведения проектной оценки надежности решает задачу автоматизации процесса проведения расчетов, облегчает подготовку документа "Проектная оценка надежности" (РД50-34.698-90, пункт 2.10) благодаря возможности вывода результатов моделирования и расчетов в файл. Используемый в ПК "АРБИТР" графический аппарат схем функциональной целостности для описания структуры и взаимодействия элементов системы является логически универсальным за счет использования логических связей "И", "ИЛИ", "НЕ". Схемы функциональной целостности позволяют корректно представлять как все традиционные виды структурных схем (блок-схемы, деревья отказов, деревья событий, графы связности с циклами), так и принципиально новый класс немонотонных (некогерентных) структурных моделей различных свойств исследуемых систем.

На рисунке 1 приведен интерфейс ПК "АРБИТР" после выполнения расчета надежности системы электроснабжения (СЭС) кольцевой структуры, состоящей из трех генераторов одинаковой мощности, трех главных распределительных щитов (ГРЩ), трех перемычек, шести вторичных распределительных щитов (ВРЩ). СЭС предназначена для обеспечения бесперебойного питания одновременно трех групп потребителей (П1, П2, П3). Мощность каждого генератора достаточна для обеспечения работы всех потребителей. Ограничения по пропускной способности ГРЩ и перемычек отсутствуют. Впервые эта задача была рассмотрена в [1].

В настоящее время СФЦ широко применяются при построении структурных схем для расчета показателей надежности, безопасности, стойкости, живучести, технического риска структурно-сложных технических систем.

АО "СПИК СЗМА" с 2001 года выполняет проектные оценки надежности в полном соответствии с серией стандартов "Надежность в технике", в том числе [9, 10]. За это время выполнено более 60 проектных оценок надежности как при выполнении своих проектов, так и по договорам подряда для проектов, разработанных сторонними организациями. В настоящее время ПК "АРБИТР" используется в 12 высших учебных заведениях Российской Федерации, в 10 научно-исследовательских институтах и центрах, в 12 проектных организациях и предприятиях промышленности.

ОБОСНОВАНИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ПАЗ

С помощью ПК “АРБИТР” могут быть решены задачи, связанные с расчетом риска аварий на опасных производственных объектах (ОПО) и показателей функциональной безопасности (ФБ) систем противоаварийной автоматической защиты (систем ПАЗ).

Требования, определяющие необходимость решения данных задач, приведены в федеральном законе ФЗ №116 от 21.01.1997 “О промышленной безопасности опасных производственных объектов” и в Федеральных нормах и правилах (ФНиП) Ростехнадзора в области промышленной безопасности. Так, например, требование о необходимости проектного обоснования выбора систем ПАЗ на основании анализа опасностей и оценки риска аварий приведено в п. 2.1 ФНиП “Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств” (далее – “ОПВБ”). Указанное требование выполняется с учетом Приказа Ростехнадзора №144 от 11.04.2016 г. об утверждении Руководства по безопасности “Методические основы по проведению анализа опасностей и оценки риска аварий на ОПО” (далее – Руководство), в котором представлены основные методы анализа опасностей и оценки риска аварий на ОПО. В Руководстве отмечено, что при анализе опасностей, связанных с отказами технических устройств систем ПАЗ, оценивается технический риск, показатели которого определяются соответствующими методами теории надежности. Методы расчета надежности технических систем рекомендуется сочетать с методами моделирования аварий и количественной оценкой риска аварий.

В настоящее время наиболее распространенными методами анализа риска аварий являются: качественный метод “Анализ опасности и работоспособности” (HAZOP, ГОСТ Р 51901.11–2005); полуколичественный метод “Анализ вида, последствий и критичности отказа” (FMECA, ГОСТ 27.310–1995); качественный/количественный метод “Анализ деревьев отказов” (FTA, ГОСТ Р 51901.13-2005); количественный метод “Анализ дерева событий” (ETA, ГОСТ Р МЭК 62502-2014). ПК “АРБИТР” позволяет проводить анализ и расчет риска с использованием всех вышеуказанных методов.

Рассмотрим более подробно требования, предъявляемые к функциональной безопасности систем ПАЗ для нефтехимических и нефтеперерабатывающих объектов, указанные в ОПВБ.

Согласно пункту 6.3.4 ОПВБ 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 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. Далее, в пункте 6.3.5 ОПВБ указано, что *методы создания систем ПАЗ должны определяться на основании анализа опасности и работоспособности контуров безопасности с учетом риска, возникающего при отказе контура безопасности. И, кроме того, согласно пункту 6.3.21 показатели надёжности систем ПАЗ устанавливаются и проверяются не менее чем для двух типов отказов данных систем: отказы типа “несрабатывание” и отказы типа “ложное срабатывание”.*

Порядок и методы выполнения требований к системам ПАЗ для непрерывных производственных процессов отражен в ГОСТ Р МЭК 61511 “Безопасность функциональная. Системы безопасности приборные для промышленных процессов”. В ГОСТ Р МЭК 61511 понятие функциональной безопасности определяется как часть безопасности процесса, которая зависит от правильного функционирования системы ПАЗ и других слоев защиты. После проведения идентификации опасностей процесса и оценки рисков, связанных с ними, стандарт предлагает проводить процедуру распределения рисков по слоям защиты, которые предотвращают или снижают эту опасность (метод LOPA). По результатам анализа снижения риска каждым слоем защиты, определяется общая мера снижения риска, и рассматривается необходимость его дальнейшего снижения. Если принимается решение о необходимости дальнейшего снижения риска путем введения дополнительного слоя защиты в виде контура безопасности ПАЗ, то метод анализа слоев защиты позволяет определить соответствующий этой функции уровень полноты безопасности (УПБ/SIL).

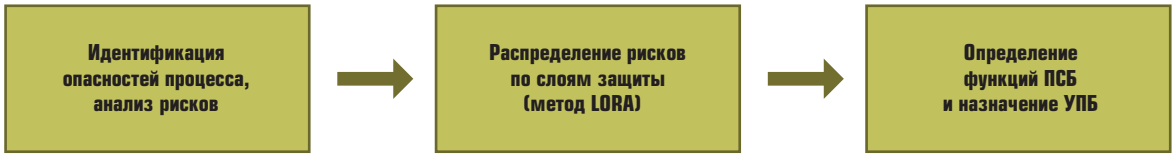

Рис. 2. Схема назначения УПБ функций безопасности ПАЗ

На рисунке 2 приведена схема формирования требований к УПБ функций безопасности ПАЗ, согласно ГОСТ Р МЭК 61511.

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.

Назначенный УПБ определяет требования к отказоустойчивости и надежности функционирования контура безопасности системы ПАЗ, требования к мерам по снижению систематических отказов. Требование к отказоустойчивости (резервированию) определяет минимальное количество отказов в контуре безопасности, при котором контур все еще может выполнять свою функцию. Значения минимально допустимого числа отказов и требования к надежности контуров ПАЗ, в зависимости от назначенных для них УПБ, приведены в таблице 1. Для функций безопасности, работающих в режиме редких запросов, в качестве характеристики надежности контура используется средняя вероятность отказа выполнения по запросу (PFDavg). Для функций безопасности, работающих в режиме непрерывных запросов – средняя частота отказов в час.

Таким образом, оценка функциональной безопасности системы ПАЗ заключается в документальной проверке соответствия контуров системы ПАЗ установленным для них уровням полноты безопасности на основании анализа опасностей, рисков и слоев защиты. Проектную оценку функциональной безопасности можно проводить на этапе разработки проекта системы ПАЗ. Если на этапе проектирования оценка функциональной безопасности не проводилась, то возможно проведение оценки функциональной безопасности после монтажа системы на объекте и после получения опыта эксплуатации и обслуживания. Рекомендуется проводить оценку функциональной безопасности после проведения изменений и перед выводом системы ПАЗ из эксплуатации. Для проведения проектной оценки функциональной безопасности необходимо, чтобы техническое задание на создание системы ПАЗ содержало перечень контуров безопасности с назначенными УПБ.

Вероятность отказа выполнения по запросу (PFDavg) рассчитывается для каждого контура ПАЗ, так как им могут быть свойственны различные виды отказов компонентов и архитектур ПАЗ в части резервирования. Графические и вычислительные средства ПК “АРБИТР” представляют собой мощный и удобный в инженерном смысле слова инструмент для автоматизированного расчета показателей надежности и функциональной безопасности систем ПАЗ. Для подготовки исходных данных для элементов ПАЗ используется встроенная утилита, позволяющая рассчитать показатели PFDavg для базовых структур 1oo1

Таблица 1. Требования к отказоустойчивости и надежности контура безопасности

УПБ	Режим запросов	Минимально допустимое число отказов	Средняя вероятность отказа выполнения по запросу	Средняя частота отказов в час
1	любой	0	$10^{-2} – 10^{-1}$	$10^{-6} – 10^{-5}$
2	редкие запросы	0	$10^{-3} – 10^{-2}$	$10^{-7} – 10^{-6}$
	частые/непрерывные	1		
3	любой	1	$10^{-4} – 10^{-3}$	$10^{-8} – 10^{-7}$
4	любой	2	$10^{-5} – 10^{-4}$	$10^{-9} – 10^{-8}$

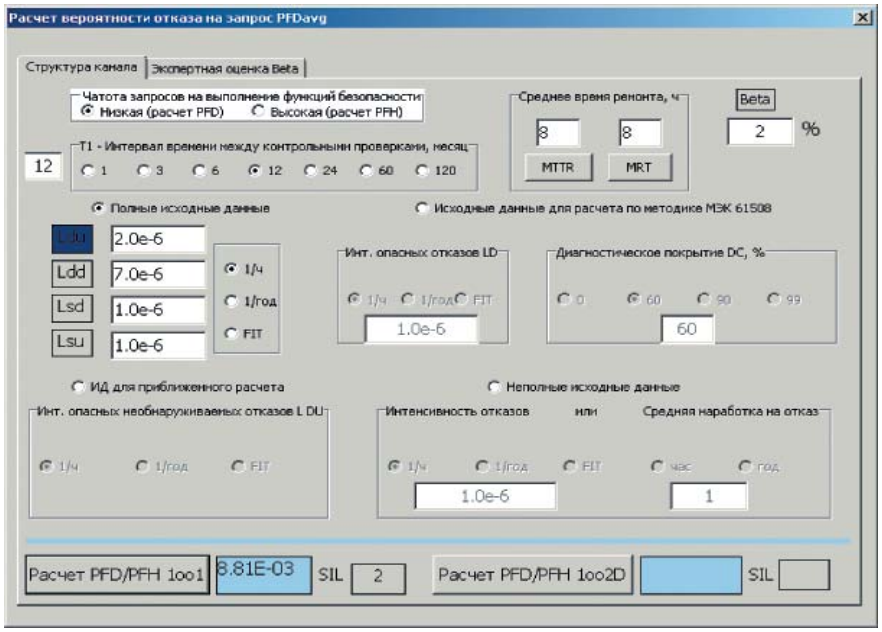

Рис. 3. Интерфейс встроенной в ПК "АРБИТР" утилиты для расчета PFDavg

и 1oo2D. Интерфейс утилиты показан на рисунке 3. Дальнейшее моделирование и расчет показателей надежности контуров систем ПАЗ осуществляется в ПК "АРБИТР" на основе данных, подготовленных утилитой.

Таким образом, согласно действующим нормативным требованиям при проектировании систем ПАЗ должно выполняться следующее:

- проведение анализа опасности процесса с учетом риска аварий на ОПО, возникающего при отказе контуров ПАЗ, с последующим назначением требуемых уровней SIL;
- включение в техническое задание на проектирование системы ПАЗ перечня контуров с назначенными для них уровнями SIL;
- применение в системах ПАЗ объектов, содержащих I и II блоки взрывоопасности программируемых контроллеров, имеющих сертификат соответствия требованиям ФБ;
- проведение проектной оценки функциональной безопасности системы ПАЗ, включающее подтверждение соответствия значений показателей надежности и отказоустойчивости контуров системы ПАЗ требуемым значениям, определенным согласно назначенных контурам уровней полноты безопасности.

ЗАКЛЮЧЕНИЕ

1. ФНиП в области промышленной безопасности требуют проведения анализа опасностей и оценки риска аварий, с последующей оценкой показателей надежности системы ПАЗ.
2. В техническом задании на создание системы ПАЗ должен быть приведен перечень контуров ПАЗ с назначенными им УПБ.
3. При проектировании системы ПАЗ определение структуры и выбор компонентов контуров ПАЗ должны производиться с учетом их показателей отказоустойчивости и надежности. Подтверждение соответствия проектируемой системы ПАЗ требованиям функциональной безопасности является обязательным требованием ФНиП "ОПВБ для взрывопожароопасных, нефтехимических и нефтеперерабатывающих производств".
4. В объем проектной документации на ОПО, предоставляемой на государственную экспертизу и на экспертизу промышленной безопасности, должен быть включен специальный раздел, содержащий следующие документы:
   - "Отчет о проведении анализа опасностей и оценки риска", содержащий, например, результаты проведения процедуры (HAZOP).
   - "Отчет о назначении уровней полноты безопасности 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 (SIL).

- "Проектная оценка функциональной безопасности", содержащая подтверждение соответствия значений показателей надежности и отказоустойчивости контуров системы ПАЗ назначенным для них УПБ (SIL).

Список литературы

1. *Рябинин И.А.* Основы теории и расчета надежности судовых электроэнергетических систем. — Л.: Судостроение, 1967, 362 с.
2. *Рябинин И.А.* Логико-вероятностные методы исследования надежности структурно-сложных систем. — М.: Радио и связь, 1981, 264 с.
3. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем. СПб.: Издательство Санкт-Петербургского университета, 2007, 278 с.
4. *Можаев А.С.* Технология автоматизированного структурно-логического моделирования надежности, живучести, безопасности, эффективности и риска функционирования систем / А.С. Можаев // Приборы и системы, Управление, Контроль, Диагностика. – Спб., ООО Издательство "Научтехлитиздат", 2008, № 9/2008, с. 1-14.
5. *Можаев А.С.* Универсальный графоаналитический метод, алгоритм и программный модуль построения монотонных и немонотонных логических функций работоспособности систем. // Труды Международной научной школы: "Моделирование и анализ безопасности, риска в сложных системах" (МАБР– 2003). СПб.: СПбГУАП, 2003, с. 101-110.
6. *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.
7. *Нозик А.А., Струков А.В., Можаева И.А.* "Программная реализация методов количественного анализа риска аварий опасных производственных объектов на основе логико-вероятностного и логико-детерминированного подходов"/"Наука и безопасность". 2016, № 2/20.
8. *Гладкова И.А., Можаев А.С., Нозик А.А., Струков А.В.* Применение ПК "АРБИТР" в задачах проектной оценки надежности структурно-сложных систем // Сборник докладов международного научного семинара им. Ю.Н. Руденко "Методические вопросы исследования надежности больших систем энергетики", выпуск 65, Иркутск, 2015 г.
9. *ГОСТ 27.301-95.* Надежность в технике. Расчет надежности. Основные положения.
10. *ГОСТ 27.002-2015.* Надежность в технике (ССНТ). Термины и определения.

Скворцов Михаил Сереевич *– канд. техн. наук, ведущий инженер-программист, АО "СПИК СЗМА".*