

Применение автоматизированного структурно-логического моделирования для проектного расчета надежности АСУ

**А.С. Можаяев,
М.С. Скворцов,
А.В. Струков**
/ОАО "СПИК СЗМА",
г. Санкт-Петербург/

Введение

Расчет надежности как процедура определения значений показателей надежности (ПН) объекта с использованием методов, основанных на их вычислении по справочным и другим данным о надежности элементов объекта, имеющихся к моменту расчета [2], входит в состав обязательных работ по обеспечению надежности любой автоматизированной системы управления (АСУ). Общий порядок расчета надежности АСУ учитывает тот факт, что любая АСУ является многофункциональной системой, функции которой имеют различную значимость и характеризуются разным уровнем требований к надежности их выполнения [1, 4].

Построение расчетной модели для оценки показателей надежности осуществляется для каждой функции АСУ в отдельности. Основными методами расчета ПН АСУ являются структурные, основанные на представлении объекта в виде логической (структурно-функциональной) схемы [2]. В качестве исходных данных используется информация о надежности элементов, их структурных и функциональных связях и особен-

ностях режимов эксплуатации элементов, подсистем и системы в целом.

В статье описывается методика применения современной технологии автоматизированного структурно-логического моделирования (АСМ), реализованной в программном комплексе "Арбитр" [6], приводятся примеры расчета надежности элементов АСУТП нефтеперерабатывающего предприятия.

Общий порядок оценки надежности АСУ

Проектная оценка надежности АСУ осуществляется на этапах эскизного, технического или рабочего проектирования и оформляется в виде документа "Проектная оценка надежности системы" (код документа - Б1) [3].

Поскольку проектная оценка надежности АСУ, как правило, проводится на ранних этапах разработки системы, расчеты ведутся главным образом только с учетом свойств комплекса технических средств (КТС). При этом оценка надежности АСУ является ориентировочной и служит для решения задач повышения надежности функционирования

технического и программного обеспечения системы [1].

Структурные методы расчета ПН применяются прежде всего для объектов, поддающихся разукрупнению на элементы, характеристики надежности которых известны на момент проведения расчетов. Элементом АСУ является отдельная относительно самостоятельная часть системы, участвующая в реализации одной или нескольких функций АСУ и рассматриваемая при решении задач надежности как не разложимая на составляющие.

Функцией автоматизированной системы является совокупность действий АСУ, направленная на достижение определенной цели. Установление требований к надежности разрабатываемой (модернизируемой) АСУ проводят по каждой функции системы [1].

Для описания надежности АСУ по непрерывно выполняемым функциям (Н-функциям) и по дискретно выполняемым функциям (Д-функциям) используются различные показатели надежности, как единичные, так и комплексные. В табл. 1 представлены показатели надежности по указанным типам функций [1].

При проведении проектной оценки надежности АСУ используются исходные данные:

- о надежности элементов АСУ;
- о структурных и функциональных связях элементов АСУ;
- об особенностях режимов эксплуатации элементов, подсистем и системы в целом.

Исходные данные о показателях надежности элементов АСУ приводятся в документации их изготовителей и разработчиков, в официальных отчетах об эксплуатации элементов АСУ, а также в справочниках и на официальных интернет-сайтах производителей комплектующих изделий и элементов.

Исходные данные могут приводиться как в виде значений интенсивностей отказов λ (Failure Rate), так и в виде средней наработки между отказами (MTBF - Mean Time Between Failures) для восстанавливаемых изделий или средней наработки до (первого) отказа (MTTF - Mean Time to Failure) для невозстанавливаемых изделий. Наиболее часто при проектной оценке надежности АСУ принимается гипотеза о постоянной интенсивности отказов или экспоненциальном распределении наработки между

отказами. В этом случае показатели надежности элементов связаны отношением $\lambda = 1/MTBF$, а пересчет в значения вероятностей безотказной работы на заданном интервале времени (обычно 1 год или 24 часа) осуществляется по формуле

$$P(t) = \exp(-t/MTBF) = \exp(-\lambda t).$$

В табл. 2 приведен фрагмент исходных данных по составу АСУ и параметрам надежности ее элементов.

Для построения расчетной модели надежности необходимо систематизировать информацию о конкретных конструкторских решениях по каждой функции АСУ, что требует изучения значительного объема проектной документации. Опыт проведения компанией ОАО "СПИК СЗМА" проектной оценки надежности по заданию разработчика АСУ показал, что содержание документов существенно зависит от особенностей создаваемой АСУ, объема и стадии проектирования (системы, подсистемы и т.д.). В компании был сформирован предварительный перечень документов (фрагментов документов), необходимых на



Таблица 1

Показатели надежности АСУ	
Непрерывно выполняемые функции (Н-функции)	Дискретно выполняемые функции (Д-функции)
Основные единичные показатели надежности Безотказность Средняя наработка на отказ Вероятность безотказного выполнения функции Дополнительные единичные показатели надежности Средняя наработка до отказа Параметр потока отказов системы Интенсивность отказов системы Комплексные показатели надежности Коэффициент готовности системы Коэффициент технического использования системы Коэффициент сохранения эффективности системы	Основные комплексные показатели надежности Вероятность успешного выполнения системой заданной процедуры Коэффициент оперативной готовности системы Дополнительные комплексные показатели надежности Вероятность успешного выполнения n последовательно поступивших запросов
Ремонтпригодность Среднее время восстановления Вероятность восстановления системы	

Таблица 2

Состав элементов АСУ и параметры их надежности						
№	Тип элемента АСУ	Источник	T_{oi} (год)	λ (* 10 ⁶ ч)	P (t = 1 год)	P (t = 24ч)
1	Контроллер CPU 417H v4	Фирма-производитель Siemens	30,0	3.8	0.967	0.99991
...
14	Барьер MTL4546	Фирма-производитель MTL	112,4	1.0	0.991	0.99998
...
27	Датчик уровня Model 2120	Rosemount www.emersonprocess.com/rosemount/solution000...pdf	38,2	2.99	0.974	0.99993



Рис. 1. Общая структурная схема АСУТП

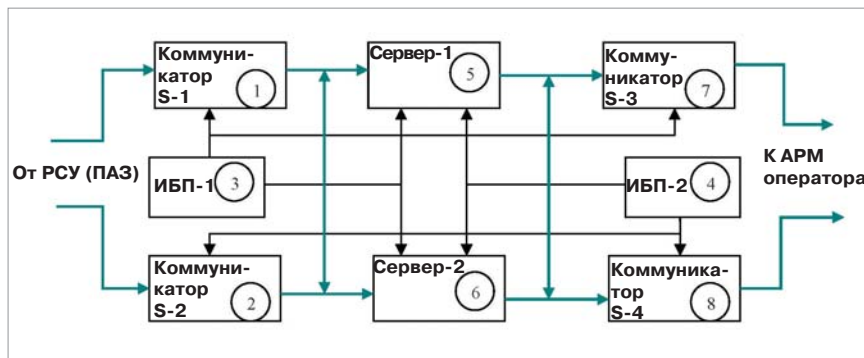


Рис. 2. Функциональная схема надежности сетевого и серверного оборудования

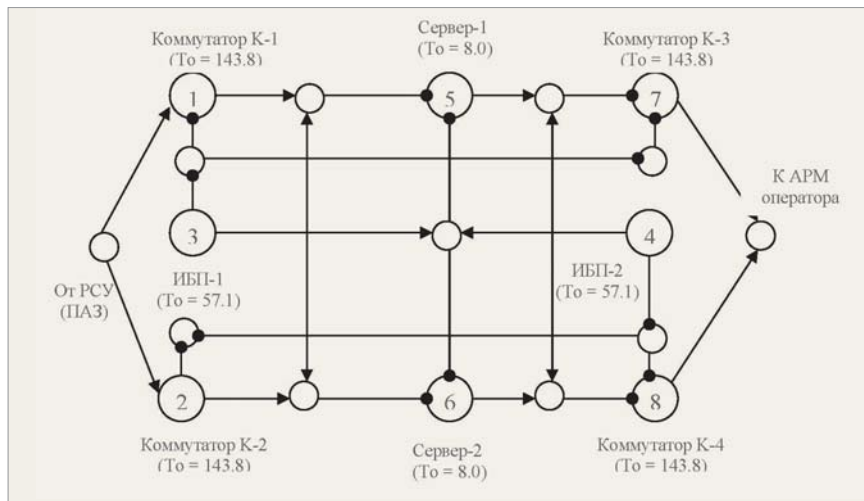


Рис. 3. Схема функциональной целостности ССО проекта АСУ

начальном этапе работ по проектной оценке надежности АСУ [5].

При построении расчетных моделей для каждого показателя надежности АСУ в первую очередь следует учитывать типовые технические требования к проектированию АСУ. К ним могут относиться требования обеспечения резервирования источников бесперебойного электропитания, отсутствия в коммуника-

ционной сети единичных точек отказа, резервирования всех контроллеров технологического процесса и коммуникационных интерфейсов, выходных плат в контурах регулирования и защиты, входных плат критически важных контуров регулирования, всех источников питания контроллеров, модулей ввода/вывода, барьеров искрозащиты, датчиков и т.д.

При построении расчетных моделей в виде структурно-функциональных схем следует выделить следующие группы (подсистемы) технических средств АСУ:

- 1) полевое оборудование (датчики, исполнительные механизмы, соединительные коробки);
- 2) средства ввода-вывода аналоговых и дискретных сигналов и их источники питания;
- 3) программно-логические контроллеры и их источники питания;
- 4) коммуникационная сеть и ее источники питания;
- 5) оборудование рабочих станций.

Общий вид структурной схемы для проектного расчета надежности АСУТП представлен на рис. 1.

Практическая реализация технологии АСУ как структурного метода проектной оценки надежности АСУ включает в себя следующие последовательные этапы [2, 5].

Представление объекта в виде логической (структурно-функциональной) схемы. На этом этапе на основе технической документации проекта АСУ строятся функциональные схемы надежности (работоспособности, отказа) для каждой исследуемой функции. Функциональные схемы разрабатываются либо разработчиком проекта АСУ, либо сторонним исполнителем проектного расчета надежности с обязательным согласованием с разработчиком проекта.

Формирование в программном комплексе структурных моделей надежности с помощью специального аппарата схем функциональной целостности (СФЦ), который является графическим интерфейсом для построения логико-вероятностной модели надежности исследуемой функции.

Процедуры построения структурно-функциональных схем и схем функциональной целостности являются ручными и не поддаются полной формализации. Они выстраиваются на основе знаний специалистов о составе элементов, режимах работы и параметрах элементов, условиях выполнения заданных функций исследуемой АСУ.

Расчет системных показателей надежности. На данном этапе пользователь вводит исходные данные и определяет перечень оцениваемых ПН. Построение

математических моделей, позволяющих в рамках введенных предположений и допущений вычислить ПН АСУ, выполняется автоматически с помощью программного комплекса "Арбитр" [6].

Анализ результатов, выработка и обоснование проектных решений. Результаты моделирования и расчета используются для содержательного анализа свойств надежности АСУ и обоснования их соответствия заданным требованиям.

На заключительной стадии проектно-го расчета надежности проводится анализ достигнутого в проекте уровня надежности реализации функций АСУ путем сравнения вычисленных показателей с типовыми нормативными требованиями к надежности АСУ.

В качестве примера в табл. 3 приведены требования к показателям надежности некоторых функций АСУ.

Пример оценки показателей надежности подсистемы АСУТП

Учитывая, что современные АСУ технологическими процессами (АСУТП) являются сложными техническими устройствами, целесообразно на начальном этапе работ по расчету надежности выделить те группы технических средств (подсистемы), которые являются общими в структурах реализации всех типов функций АСУТП. К таким подсистемам можно, например, отнести подсистему сетевого и серверного оборудования, средства АРМ оператора, подсистему питания ± 24В.

Рассмотрим порядок автоматизированного расчета показателей надежности подсистемы сетевого и серверного оборудования.

Сетевое и серверное оборудование (ССО) является общим в структурах реализации всех типов функций АСУТП. На рис. 2 приведена функциональная схема надежности подсистемы ССО проекта АСУТП [7].

В функциональной схеме ССО учтено перекрестное резервирование основного оборудования подсистемы, реализованное в проекте АСУТП. На рис. 2 цепи питания представлены тонкими черными стрелками, информационные цепи - синими стрелками. В процессе функционирования ССО сигнал от шкафов РСУ или ПАЭ через резервированные коммутаторы S-1 и S-2 (блоки 1 и 2) поступает на резервированные серверы (блоки 5 и 6) и далее через резервированные коммутаторы S-3 и S-4 (блоки 7 и 8) передается к АРМ оператора.

Приведенное выше описание требований к функционированию подсистемы ССО и составленная функциональная схема являются достаточными исходными данными для реализации следующего этапа структурно-логического моделирования - составления схемы функциональной схемы (СФЦ) с использованием ПК "АРБИТР" (рис. 3).

Функциональные вершины в СФЦ представляют состояния x_i работоспособности отдельных элементов $i=1÷8$ подсистемы ССО. Фиктивные вершины не представляют элементов системы и используются для удобства графическо-

го представления логических связей и отношений элементов в структуре.

Исходящими из вершин дугами в СФЦ представляются условия реализации собственных выходных функций элементами системы, обозначенными на схеме номерами $i=1÷8$.

На рис. 3 представлена СФЦ подсистемы ССО с указанием названий элементов и их показателей надежности (средней наработки до отказа в годах). Структура, представленная на рис. 5, относится к сложным и не может быть представлена последовательно-параллельным соединением элементов. Получение точного аналитического выражения для оценки вероятности безотказной работы такой системы является весьма трудоемким процессом.

Программный комплекс "Арбитр" автоматически формирует многочлен вероятностной функции. Для подсистемы ССО такой многочлен имеет вид:

$$P_{ССО} = P_{К-1} R_{ИБП-1} P_{Сервер-1} P_{К-3} + Q_{К-1} P_{К-2} R_{ИБП-1} R_{ИБП-2} P_{Сервер-1} P_{К-3} Q_{К-4} + Q_{К-1} P_{К-2} R_{ИБП-1} R_{ИБП-2} Q_{Сервер-1} P_{Сервер-2} P_{К-3} Q_{К-4} + P_{К-1} R_{ИБП-1} Q_{Сервер-1} P_{Сервер-2} P_{К-3} + P_{К-2} R_{ИБП-2} P_{Сервер-2} P_{К-4} + P_{К-1} Q_{К-2} R_{ИБП-1} R_{ИБП-2} P_{Сервер-2} Q_{К-3} P_{К-4} + P_{К-1} Q_{К-2} R_{ИБП-1} R_{ИБП-2} P_{Сервер-1} Q_{Сервер-2} Q_{К-3} P_{К-4} + P_{К-2} R_{ИБП-2} P_{Сервер-1} Q_{Сервер-2} P_{К-4} - P_{К-1} P_{К-2} R_{ИБП-1} R_{ИБП-2} Q_{Сервер-1} P_{Сервер-2} P_{К-3} P_{К-4} - P_{К-1} P_{К-2} R_{ИБП-1} R_{ИБП-2} P_{Сервер-1} Q_{Сервер-2} P_{К-3} P_{К-4}, \quad (1)$$

Таблица 3

Нормативные показатели надежности АСУ

Тип функции	Название основного показателя надежности	Нормативное значение
Функции F1 - контроля и информационные функции	Коэффициент готовности ($T_{Bi} \leq 1$ час)	≥ 0.99
Функции F2 - регулирования и автоматического управления	Вероятность безотказной работы ($t = 8760$ час)	≥ 0.9
Функции F3 - системы безопасности и противоаварийной защиты	Коэффициент оперативной готовности	≥ 0.999

Таблица 4

Показатели надежности элементов подсистемы ССО

Наименование оборудования	Схемные обозначения	T_{oi} (год)	P_i (t=1 год)	TBi (час)
Коммутатор	S-1, S-2, S-3, S-4	143.8	0.9931	8.0
ИБП	ИБП-1, ИБП-2	57.1	0.9826	8.0
Сервер	Сервер-1, -2	8.0	0.8825	8.0

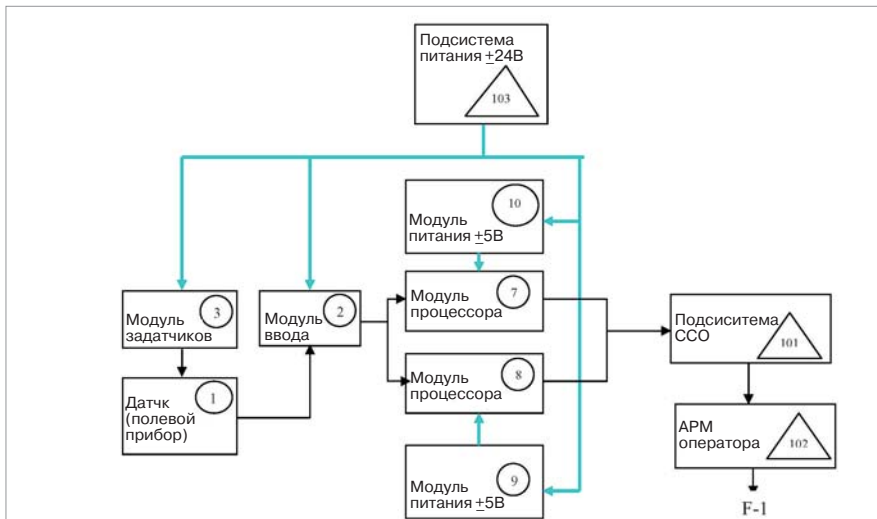


Рис. 4. Упрощенная структурная схема реализации функции F1

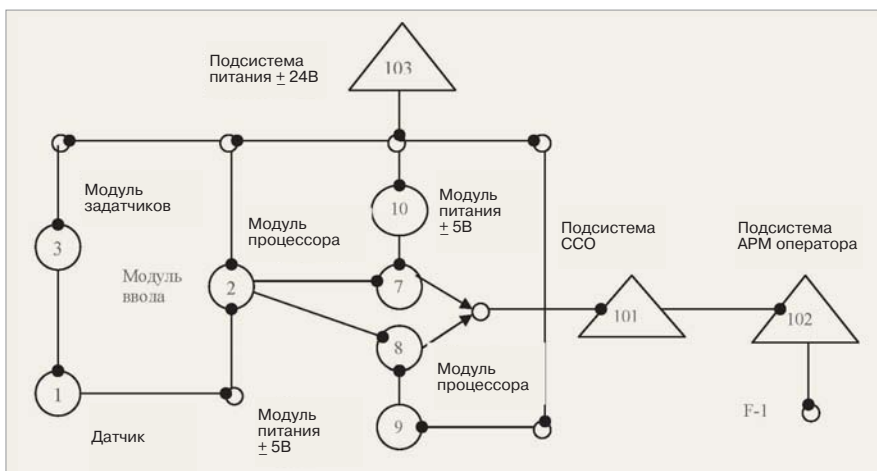


Рис. 5. Схема функциональной целостности для функции F1

дежности рассчитывался коэффициент готовности КГ. Результаты, приведенные в табл. 5, могут быть использованы для оценки как достигнутого уровня надежности, так и влияния организации системы эксплуатации (ремонта) на надежность проектируемой подсистемы.

Пример оценки показателей надежности выполнения простой функции

Для выполнения проектной оценки показателей надежности АСУ по заданной функции необходимо преобразовать общую структурную функцию (рис. 1) с учетом номенклатуры и взаимосвязей конкретных элементов, задействованных в реализации этой функции.

На рис. 4 представлена упрощенная структурная схема реализации информационной функции F1 [7]. На схеме прямоугольниками представлены основные элементы и подсистемы АСУТП, безотказная работа которых обеспечивает реализацию информационной функции F1. Всем элементам структурной схемы на рис. 4 сопоставлены их собственные номера (записаны в кружках). Номера подсистем записаны в треугольниках (эквивалентированных вершинах) - это указывает на тот факт, что сами подсистемы имеют собственную структуру, как было показано на примере подсистемы сетевого и серверного оборудования. Эти номера далее используются для обозначения элементарных событий безотказной работы соответствующих элементов и подсистем в математических моделях надежности, формируемых программным комплексом АРБИТР.

На рис. 4 цепи питания представлены тонкими черными стрелками, информационные цепи - утолщенными синими.

На рис. 5 приведена структурная модель работоспособности (безотказности) реализации функции F1 АСУТП в форме схемы функциональной целостности (СФЦ). Она используется для автоматизированного моделирования и расчета по-

где P_{CCO} - вероятность безотказного выполнения функции подсистемой ССО;
 P_{xxx} - заданная вероятность безотказной работы xxx-элемента;
 $Q_{xxx}=1-P_{xxx}$ - вероятность отказа xxx-элемента.

Для случая равнонадежных элементов полином (1) имеет вид

$$P_{CCO} = 4P^4 + 2P^5 - 10P^6 + 6P^7 - P^8. \quad (2)$$

В табл. 4 приведен пример исходных данных для расчета показателей надежности ССО с использованием ПК "Арбитр". Исходные данные по безотказности могут вводиться либо в виде средней наработки до отказа T_{oi} (в годах), либо в величинах вероятности безотказной ра-

боты P_i . Показатели ремонтпригодности элементов задаются в виде среднего времени восстановления T_{B_i} (в часах). Для проектной оценки надежности АСУ принимается допущение об экспоненциальном законе распределения времени восстановления и времени наработки до отказа элементов.

В табл. 5 приведены результаты расчета показателей надежности подсистемы ССО в режимах с восстановлением и без восстановления.

Вероятность безотказного выполнения функции подсистемой P_{CCO} рассчитывалась для интервала эксплуатации $t=1$ год. В качестве комплексного показателя на-

Таблица 5

Результаты проектной оценки показателей надежности подсистемы ССО

Тип восстановления	$P_{CCO}(t=1 \text{ год})$	T_o (год)	K_G	T_B (час)
Восстанавливаемая	0.99997	33 157.8	0.999 999 986	4.0
Невосстанавливаемая	0.9853	11.1	-	-

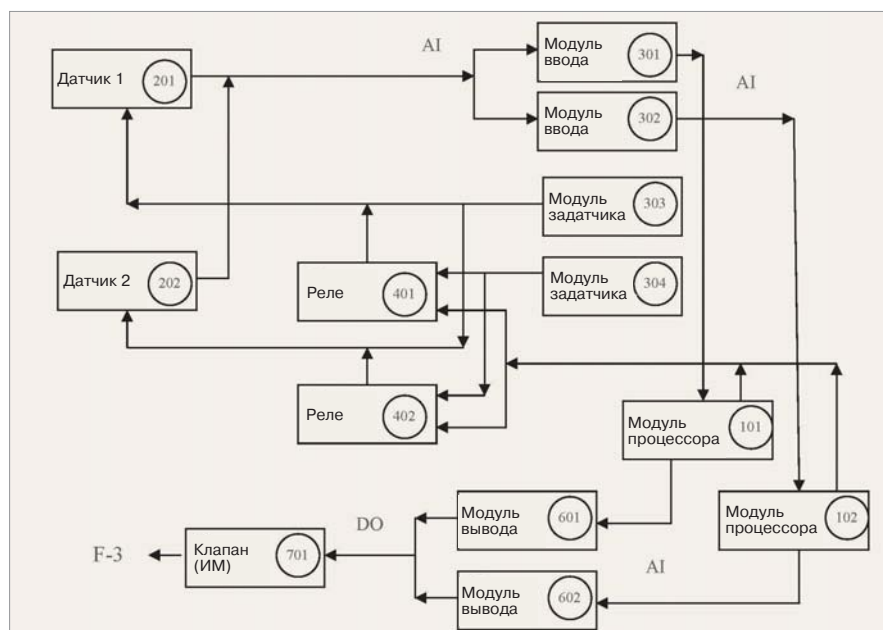


Рис. 6. Упрощенная структурная схема реализации функции F3

Таблица 6

Кратчайшие пути успешного функционирования				
№ КПУФ	ФРС			
	Модули	Блок процессоров	Подсистемы	
1	X1 X2X3	X7	X10	X101 X102 X103
2	X1 X2 X3	X8	X9	X101 X102 X103

казателей надежности в комплексе АР-БИТР.

Автоматизированное моделирование и расчет с помощью программного комплекса АРБИТР показателей надежности АСУТП по реализации информационной функции F-1 показывают, что логическая функция работоспособности (ФРС) с учетом декомпозиции подсистем состоит из двух кратчайших путей успешного функционирования (КПУФ). Табличная запись ФРС приведена в табл. 6.

В табл. 6 через X_i обозначено состояние i -элемента, который может находиться в состоянии либо работоспособности ($X_i=1$), либо отказа ($X_i=0$).

Из рис. 4 и 5, а также табл. 6 видно, что структурная модель для расчета показателей надежности АСУТП по информационной функции представляется последовательно-параллельной схемой. Простота графического представления структуры и логической функции достигается за счет применения метода эквивалентирования - представления некоторых структур (подсистем) в виде эквивалентированных вершин.

Пример оценки показателей надежности выполнения сложной функции

Рассмотрим фрагмент схемы реализации функции блокировки F-3 по значениям параметров (по аналоговым сигналам) технологического процесса [7].

Упрощенная структурная схема реализации функции блокировки F-3 без цепей питания представлена на рис. 6. Аналоговые сигналы AI с выходов датчиков D1, D2 поступают через устройства ввода (номера 301, 302) на входы соответствующих модулей процессоров. Формирование сигналов управления DO на вход клапана (исполнительного механизма, номер 701) происходит в модулях вывода (номера 601, 602) по команде соответствующего контроллера. Если основным является модуль процессора первого канала (номер 101), то сигналы OPV с выхода модуля задатчиков (номер 303) поступают на датчики D1, D2 через нормально замкнутые контакты реле (номера 401, 402). В этом режиме отказы реле не приводят к отказу питания OPV датчиков.

В случае собственных или функциональных отказов модулей ввода или вывода основным становится резервный модуль процессора (номер 102). Тогда сигнал OPV с выхода модуля задатчиков (номер 304) через нормально замкнутые контакты реле (номер 402) поступает на датчики по команде резервного модуля процессора (номер 102).

В СФЦ на рис. 7 функциональными вершинами с номерами элементов представлены события безотказной работы элементов АСУТП, участвующих в реализации функции F3.

Фиктивные вершины (без номеров) использованы для удобства графического отображения логических условий выполнения функции F-3. Стрелки с острыми концами обозначают логическое условие "ИЛИ", шарообразные стрелки - логическое условие "И". Кроме того, для отображения всех условий реализации функции F-3 использовался прием размножения функциональных вершин с номерами 301, 302 и 601, 602.

Автоматизированное моделирование и расчет с помощью программного комплекса АРБИТР показывают, что в данном случае логическая функция работоспособности (ФРС) состоит из двух кратчайших путей успешного функционирования (КПУФ). Табличная запись ФРС приведена в табл. 7.

Анализ записи КПУФ в табл. 7 показывает минимальный набор работоспособных элементов схемы для случаев основного и резервного модулей процессоров (X101 и X102), обеспечивающих реализацию функции F-3. При этом КПУФ №1 состоит из минимального набора работоспособных элементов для случая, когда основным является модуль процессора первого канала (номер 101), КПУФ №2 - когда основным является модуль процессора второго канала (номер 102).

В качестве численного примера расчета системных показателей надежности и анализа результатов рассмотрим случай равнонадежных элементов схемы реализации функции F3 (рис. 6). Пусть элементы схемы имеют следующие показатели надежности:

- вероятность безотказной работы на интервале $t=1$ (год) $P(t)=0.95$;

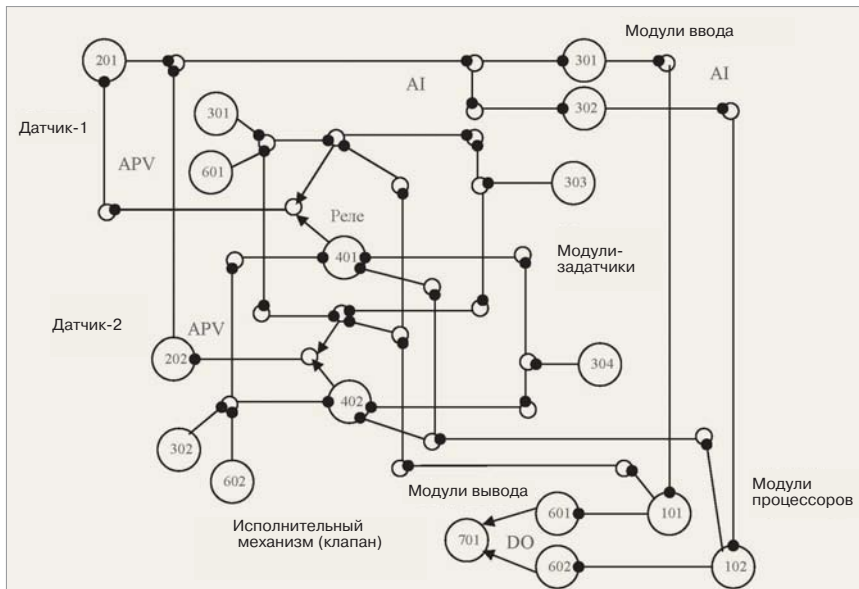


Рис. 7. СФЦ надежности реализации функции F3

Таблица 7

Кратчайшие пути функционирования для функции F-3

№ КПУФ	Датчики	Модули ввода	Модули вывода	Модули-здатчики	Модули процессоров	ИМ	Реле
1	X201 X202	X301	X601	X326	X101	X323	-
2	X201 X202	X302	X602	X327	X102	X323	X401 X402

■ среднее время восстановления $t_{в} = 8$ (час).

Результаты моделирования с использованием ПК АРБИТР:

■ стационарный коэффициент готовности - $K_g = 0,99986$;

■ вероятность безотказного выполнения функции (без восстановления) за время $t_p = 24$ (час) - $P(t_p) = 0,99958$;

■ коэффициент оперативной готовности на интервале t_p - $K_{ог}(t_p) = K_g P(t_p) = 0,99944$;

■ максимальный положительный вклад P_+ = 2,34E-005 имеют элементы с

номерах 201, 202 (датчики 1 и 2) и 701 (исполнительный механизм).

Анализ полученных результатов моделирования показывает:

1. Проектируемая АСУТП удовлетворяет нормативным требованиям (табл. 3) по надежности выполнения функции системы безопасности и противоаварийной защиты F3.

2. Максимальное увеличение показателей надежности (безотказности) возможно при увеличении показателей безотказности датчиков и исполнительного механизма (клапана).

Последний вывод сформулирован исходя из физического смысла показателя "Положительный вклад элемента P_+ ". Положительный вклад элемента характеризует увеличение безотказности невосстанавливаемой системы в случае повышения показателя безотказности элемента до 1.0.

Выводы

Изложенные в статье материалы показывают, что технология автоматизированного структурно-логического моделирования и программный комплекс АРБИТР позволяют выполнять автоматизированное моделирование и расчет показателей надежности АСУ. В 2007 году комплекс АРБИТР успешно прошел экспертизу в Совете по аттестации программных средств НТЦ ЯРБ и допущен к применению на объектах Ростехнадзора РФ. Проектный расчет надежности как вид обязательных работ по обеспечению надежности технических объектов осуществляется для каждой функции АСУ и включает в себя несколько последовательных этапов. Полнота и корректность структурно-логического моделирования предопределяются объемом и качеством представления объекта в виде логической (структурно-функциональной) схемы. Формируемый в ПК АРБИТР отчет о результатах расчета показателей надежности позволяет осуществлять не только сравнительный анализ полученных численных значений по отношению к нормативным требованиям, но и вероятностный анализ влияния показателей надежности отдельных элементов на показатели надежности всей АСУ.

Литература

- ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения.
- ГОСТ 27.301-95. Надежность в технике. Расчет надежности. Основные положения.
- ГОСТ 34.201-89. Информационная технология. Виды, комплектность и обозначение документов при создании автоматизированной системы.
- ГОСТ 27883-88. Средства измере-

- ния и управления технологическими процессами. Надежность.
5. Автоматизированные системы управления. Надежность и безопасность. Расчет надежности и безопасности автоматизированных систем управления технологическими процессами и инженерным оборудованием на стадии проектирования: Метод. рекомендации. - М.: ОАО Ассоциация "Монтажавтоматика", 2002. - 33 с.
6. АРБИТР. Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности АСУТП на стадии проектирования (ПК

- АСМ СЗМА), базовая версия 1.0. Автор: Можаяев А.С. Правообладатель: ОАО "СПИК СЗМА". Свидетельство № 2003611101 от 12 мая 2003 г. об официальной регистрации программ. Роспатент РФ, Москва, 2003. Аттестационный паспорт ПС №222 от 21 февраля 2006 г., Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) РФ.
7. Проектная оценка надежности. АСУТП "Установка очистки серосодержащих газов и производство элементарной серы". НПЗ "БОСАНСКИ БРОД" - ОАО "СПИК СЗМА", 2009. - С. 69.