

2.8. Расчет надежности системы с защитой

2.8.1. Описание задачи

Имеется система, состоящая из технического объекта и системы защиты объекта от последствий отказов его элементов. В качестве примера такого объекта может служить ядерная реакторная установка, реактор которой подлежит останову после прекращения циркуляции теплоносителя по 1 контуру, см. рис. 2.8.1.

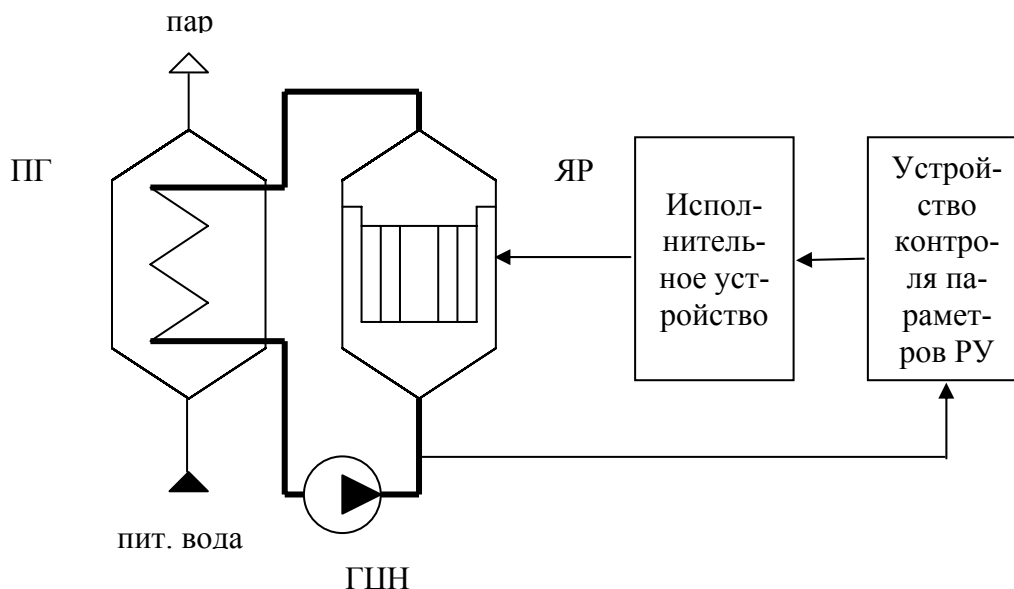


Рис. 2.8.1. Схема технического объекта с системой защиты

Степень последствий отказа такой системы зависит от того, в какой последовательности (во времени) происходят отказы ее элементов.

Так, если в момент прекращения циркуляции по 1 контуру система защиты будет работоспособна, то произойдет штатный останов ЯР и последствия отказа будут минимальны. После устранения причины прекращения циркуляции по 1 контуру ЯР может быть снова введен в действие.

В другом варианте развития аварии может сложиться такая ситуация, когда после штатного останова ЯР происходит отказ самой системы защиты. В данном случае состояние объекта защиты не ухудшится, но для ввода его в действие потребуется вначале отремонтировать систему защиты.

В третьем варианте, отказ защиты происходит до момента прекращения циркуляции по первому контуру, что приводит к невозможности заглушения реактора и, как следствие, к тяжелой аварии.

Необходимо рассчитать, с учетом последовательностей отказов элементов:

- вероятность возникновения аварии на интервале ($0 \div 10000$ ч);
- вероятность штатного останова на интервале ($0 \div 10000$ ч).

Расчет должен быть проведен при следующих исходных данных:

- интенсивность отказов устройства контроля системы защиты = $3e-6$;
- интенсивность отказов исполнительного устройства системы защиты = $5e-6$;
- интенсивность отказов Объекта = $2e-5$;
- система защиты срабатывает мгновенно.

2.8.2. Результаты решения на ПК «RELEX»

Дерево отказов для системы «Объект-Аварийная Защита», набранное в редакторе модуля Relex Fault Tree, приведено на рис. 2.8.2.

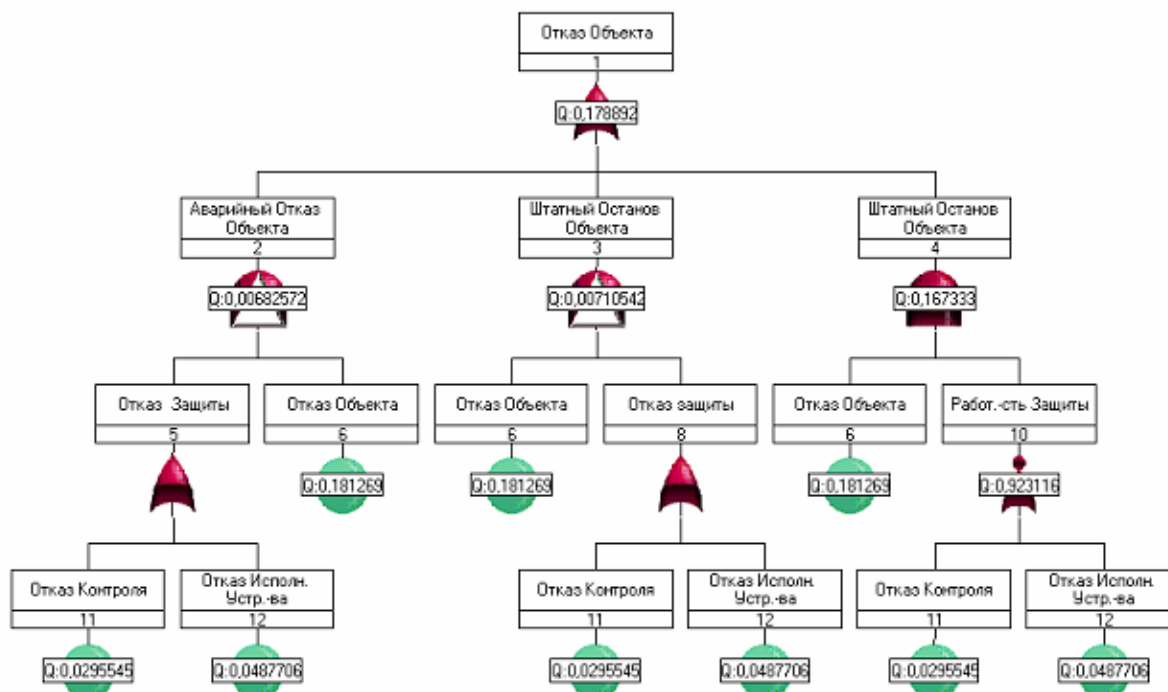


Рис. 2.8.2. Дерево отказа системы Объект+Аварийная Защита в Relex Fault Tree

В результате расчета получено:

- вероятность возникновения аварии на интервале $(0 \div 10000\text{ч}) = 0.006826$;
- вероятность штатного останова на интервале $(0 \div 10000\text{ч}) = 0.174438$.

При построении модели была учтена очередность возникновения отказов устройств системы защиты и Объекта. Для этого использовались динамические операторы дерева “приоритетное И” (см. рис.1.20), которые “срабатывают” при очередности слева - направо. Авария может возникнуть лишь при отказе объекта после отказа системы защиты. При другой последовательности (т.е. когда сначала отказывает объект), работоспособная система защиты срабатывает и осуществляет штатный безаварийный останов. В дальнейшем отказ системы защиты (если он возможен) не приведет к аварии. В данном примере предполагается, что система защиты срабатывает мгновенно. Если же требуется некоторое время для работы системы защиты и осуществления перевода всей системы (после аварийного отказа объекта) в безопасный штатный останов, то и такую модель можно построить на динамических деревьях Relex.

2.8.3. Результаты решения на ПК «АСМ»

На рис. 2.8.3 изображена СФЦ, являющаяся точным аналогом дерева отказов, приведенного на рис. 2.8.2. На этой СФЦ представлены всего три элемента исследуемой системы:

- x_6 - безотказность объекта ($\lambda_6 = 2e-5$) 1/час.;
- x_{11} - безотказность устройства контроля системы защиты ($\lambda_{11} = 3e-6$) 1/час.;
- x_{12} - безотказность исполнительного устройства системы защиты ($\lambda_{12} = 5e-5$) 1/час.

Для представления в ДО на рис. 2.8.3 (как и на рис. 2.8.2) трех вариантов отказов данной системы, выполнено размножение обозначений указанных элементов:

1. Функциональные вершины 6, 62 и 63 представляют одно событие безотказной работы объекта;
2. Функциональные вершины 11, 112 и 113 представляют одно событие безотказной работы сигнализирующего устройства контроля системы защиты;
3. Функциональные вершины 12, 122 и 123 представляют одно событие безотказной работы исполнительного устройства системы защиты

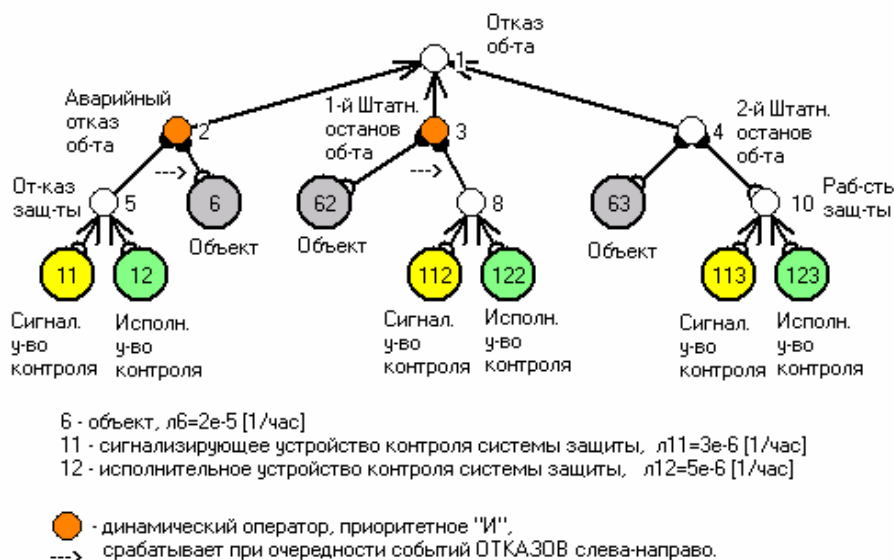


Рис. 2.8.3. СФЦ дерева отказов системы «Объект - Аварийная Защита»

Все необходимые элементарные события отказа элементов представлены в СФЦ на рис. 2.8.3 с помощью инверсных выходов связей функционального подчинения.

Как и в ДО на рис. 2.8.2, в данной СФЦ на рис.2.8.3 выделены два логических элемента (фиктивные вершины 2 и 3), с помощью которых обозначены динамические операторы "приоритетное И". Особенность этих операторов заключается в том, что при расчете вероятности $P(\tilde{y}_2)$ и $P(\tilde{y}_3)$ их выходных функциональных событий \tilde{y}_2 и \tilde{y}_3 необходимо учесть все возможные последовательности отказов обеспечивающих элементов в направлении указанном на схеме стрелкой "слева-направо". Для расчета вероятностей любых видов последовательностей отказов а технологии и ПК АСМ разработана специальная утилита, в основе которой лежит аналитический метод построения и анализа комбинаторно-последовательных логических моделей исследуемых систем.

Выполненные с использованием указанной утилиты аналитическое моделирование и расчет вероятностей заданных трех видов отказов рассматриваемой системы с защитой, на интервале 0-100000 час наработки, дал следующие результаты.

1. РАСЧЕТ ВЕРОЯТНОСТИ АВАРИЙНОГО ОТКАЗА ОБЪЕКТА

Событие аварийного отказа объекта определяется критерием y_2 . Раскрывая этот критерий на основе СФЦ, изображенной на рис. 2.8.3, определяем все составляющие его последовательности отказов sj и вычисляем их вероятности $p_{AO}(sj)$, $j = 1, 2, \dots, 6$:

Таблица 2.8.1.

Вероятности последовательностей аварийного отказа объекта		
j	sj	$p_{AO}(sj)$
1	$(\bar{x}_{11} \rightarrow \bar{x}_{12} \rightarrow \bar{x}_6)$	4.17094744319719E-5
2	$(\bar{x}_{12} \rightarrow \bar{x}_{11} \rightarrow \bar{x}_6)$	4.19159733955125E-5
3	$(\bar{x}_{12} \rightarrow \bar{x}_6 \rightarrow \bar{x}_{11})$	4.37505603666938E-5
4	$(\bar{x}_{11} \rightarrow \bar{x}_6 \rightarrow \bar{x}_{12})$	4.33153042926E-5
5	$(\bar{x}_{12} \rightarrow \bar{x}_6 \rightarrow x_{11})$	0.00418249737094801
6	$(\bar{x}_{11} \rightarrow \bar{x}_6 \rightarrow x_{12})$	0.00247587356410176

Сумма вероятностей $P_{AO}(sj)$ составляет искомую вероятность аварийного отказа объекта (вероятность возникновения аварии объекта):

$$P_C(y_2) = P_{AO}(10000) = \sum_{j=1}^6 p_{AO}(sj) = 0.00682906224753655 \quad (2.8.1)$$

Вычисленная средствами технологии АСМ вероятность (2.8.1) этого события несколько отличается от результата ее расчета, полученного с помощью модуля Relex Fault Tree, который составляет **0.0682572** (см. рис.2.8.2, "Аварийный Отказ Объекта 2").

РАСЧЕТ ВЕРОЯТНОСТИ ПЕРВОГО ШТАТНОГО ОСТАНОВА ОБЪЕКТА

Событие первого штатного останова объекта определяется критерием y_3 . Раскрывая этот критерий на основе СФЦ, изображенной на рис. 2.8.3, определяем все составляющие его последовательности отказов sj и вычисляем их вероятности $p_{1шО}(sj)$, $j = 1, 2, \dots, 4$:

Таблица 2.8.2.

Вероятности последовательностей первого штатного останова		
j	sj	$p_{1шО}(sj)$
1	$(\bar{x}_6 \rightarrow \bar{x}_{11} \rightarrow \bar{x}_{12})$	4.51794695420625E-5
2	$(\bar{x}_6 \rightarrow \bar{x}_{12} \rightarrow \bar{x}_{11})$	4.54085964162797E-5
3	$(\bar{x}_6 \rightarrow \bar{x}_{11}) \cdot x_{12}$	0.00262016293429706
4	$(\bar{x}_6 \rightarrow \bar{x}_{12}) \cdot x_{11}$	0.00439682874331591

Сумма вероятностей $p_{1шО}(sj)$ составляет искомую вероятность первого варианта штатного останова объекта:

$$P_C(y_3) = P_{1шО}(10000) = \sum_{j=1}^4 p_{1шО}(sj) = 0.00710757974357131 \quad (2.8.2)$$

Этот результат также несколько отличается от результата, полученного в Relex Fault Tree, который составляет **0.00710542** (см. рис. 2.8.2, "Штатный Останов Объекта 3).

РАСЧЕТ ВЕРОЯТНОСТИ ВТОРОГО ШТАТНОГО ОСТАНОВА ОБЪЕКТА

Событие второго штатного останова объекта определяется критерием y_4 . Это событие определяется отказом объекта (6) и безотказной работой (в течение всех 10000 час.) устройства контроля системы защиты (11) и исполнительного устройства системы защиты (12). Раскрывая этот критерий на основе СФЦ, изображенной на рис.2.8.3, определяем единственную последовательность (комбинацию) элементарных событий sj и вычисляем ее вероятность $p_{2шО}(sj)$:

Таблица 2.8.3.а.

Вероятности последовательностей второго штатного останова		
j	sj	$p_{2шО}(sj)$
1	$\bar{x}_6 \cdot x_{11} \cdot x_{12}$	0.16733260493091

Вероятность $p_{2шО}(sj)$ составляет искомую вероятность второго варианта штатного останова:

$$P_c(y_4) = P_{2шО}(10000) = p_{2шО}(sj) = 0.16733260493091 \quad (2.8.3)$$

Этот результат совпал с точностью до округления с результатом, полученным в Relex Fault Tree, который составляет **0.167333** (см. рис. 2.8.2, "Штатный Останов Объекта 4).

РАСЧЕТ ОБЩЕЙ ВЕРОЯТНОСТИ ШТАТНОГО ОСТАНОВА ОБЪЕКТА

Общая вероятность штатного останова объекта равна сумме вероятностей (2.8.2) и (2.8.3) и составляет

$$\begin{aligned} P_{шО}(10000) &= P_{1шО}(10000) + P_{2шО}(10000) = \\ &= 0.00710757974357131 + 0.16733260493091 = 0.17444018467448131 \end{aligned} \quad (2.8.4)$$

Вероятность этого события, вычисленная Relex Fault Tree, по данным, приведенным на рис.2.8.2, "Штатный останов объекта 3" + "Штатный останов объекта 4", составляет **0.17443842**, что несколько отличается от результата (2.8.4) полученного методами и средствами технологии АСМ.

РАСЧЕТ ОБЩЕЙ ВЕРОЯТНОСТИ ОТКАЗА ОБЪЕКТА

Общая вероятность отказа объекта, вычисленная средствами АСМ, равна сумме вероятностей (2.8.1) и (2.8.4)

$$\begin{aligned} Q_c(10000) &= P_{АО}(10000) + P_{шО}(10000) = \\ &= 0.00682906224753655 + 0.17444018467448131 = 0.18126924692201786 \end{aligned} \quad (2.8.5)$$

Этот результат также несколько отличается от результата Relex Fault Tree, приведенного на рис. 2.8.2 "Отказ объекта 1" и равного **0.178892**. Следует отметить, что контрольный расчет суммы вероятностей аварийного отказа и штатных остановов, выполненный по данным, указанным на рис. 2.8.2 (Relex Fault Tree) дал третий результат

$$\begin{aligned} Q_c(10000) &= 0.00682572 + 0.00710542 + 0.167333 = \\ &= 0.00682572 + 0.17443842 = 0.18126414 \end{aligned} \quad (2.8.6)$$

Однако он значительно ближе к (2.8.5).

Выяснение причин отмеченных расхождений результатов моделирования и расчетов показателей надежности систем с учетом последовательностей отказов элементов нуждается в дополнительных исследованиях.

2.8.4. Результаты решения на «RISK SPECTRUM»

Окно ПК «Risk Spectrum» с результатами моделирования и расчетов представлено на рисунках 2.8.4 -.

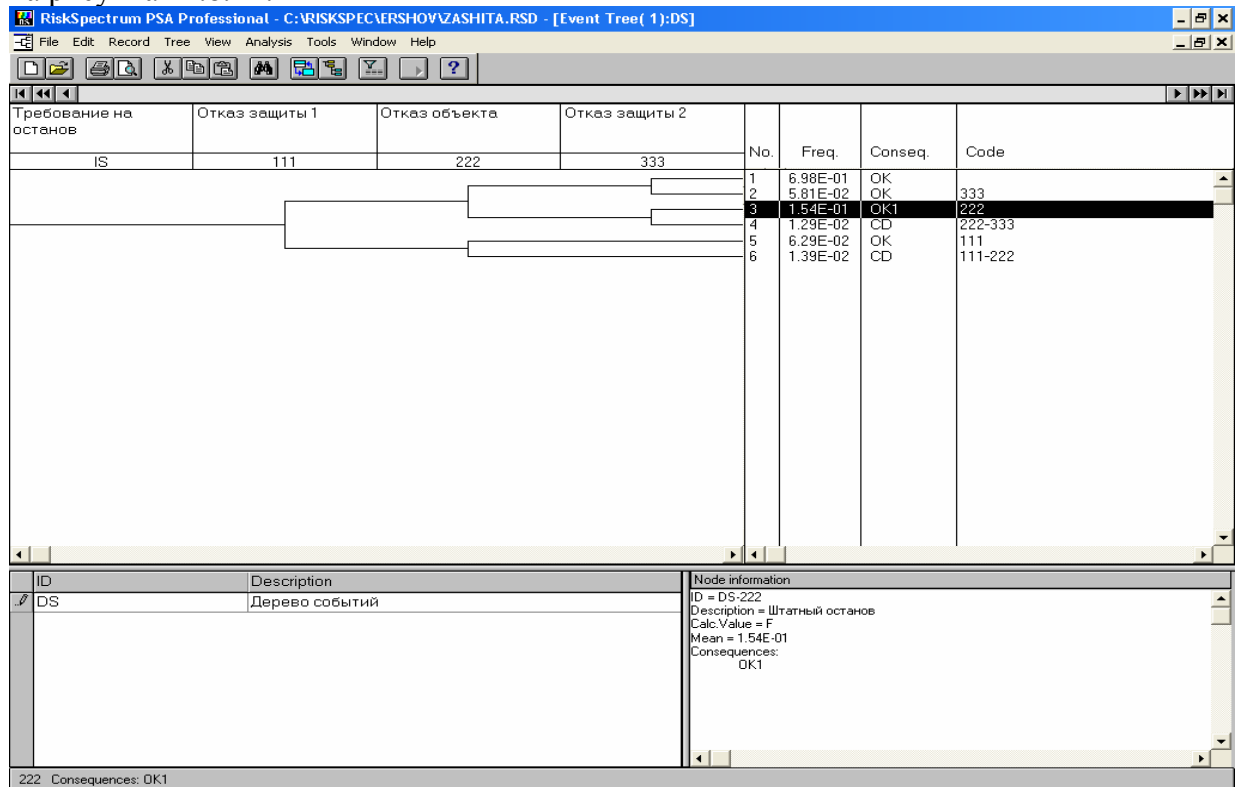


Рис. 2.8.4. Дерево событий для системы с защитой и результаты расчетов с учетом вероятности успешного срабатывания систем

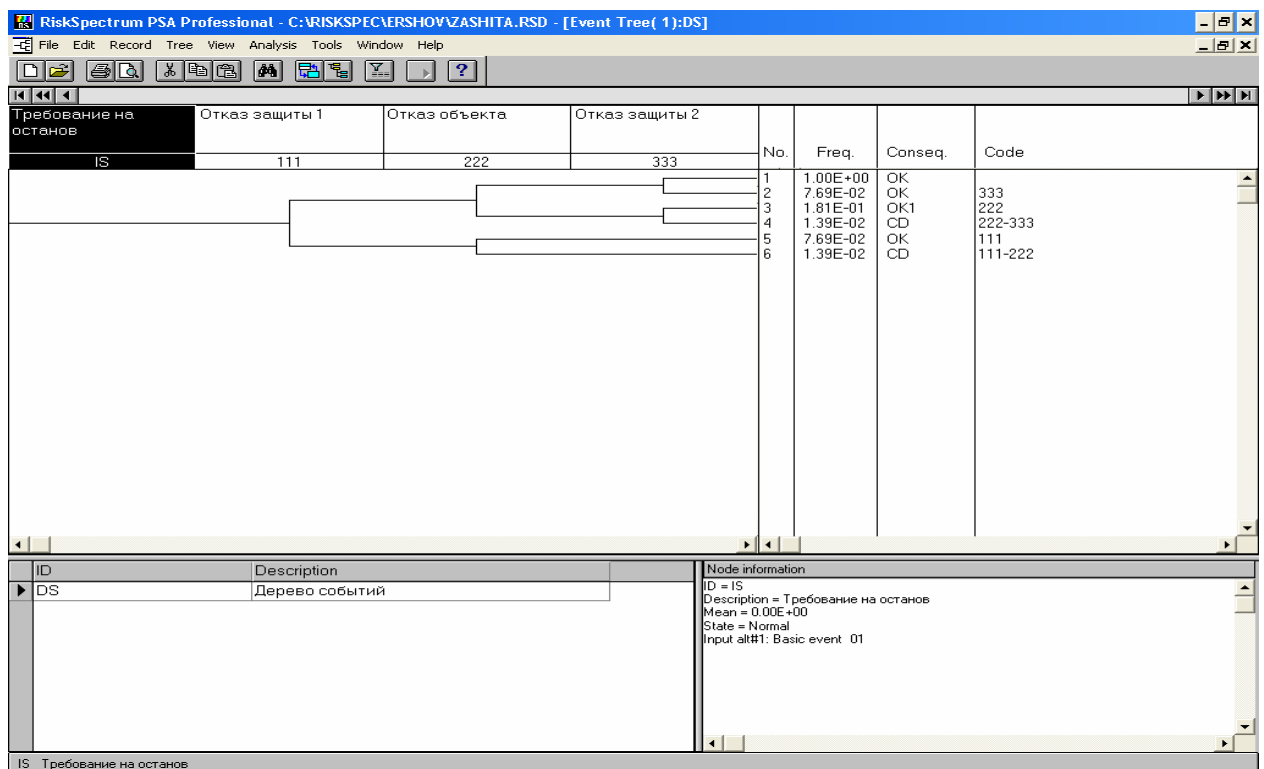


Рис. 2.8.5. Дерево событий для системы с защитой и результаты расчетов без учета вероятности успешного срабатывания систем

RiskSpectrum PSA Professional - C:\RISKSPEC\ERSHOV\ZASHITA.RSD - [Sequence Analysis Case(1):6]

File Edit Record View Analysis Tools Window Help

ID - Char. # 1	Description	Calc.type	Mean	5th perc.	Median	95th perc.	Text Result	Gate Out	BE Out	Exch
1		F	1.26E-01	1.26E-01	1.26E-01	1.26E-01	No	No	No	N
2		F	1.05E-02	1.05E-02	1.05E-02	1.05E-02	No	No	No	N
3		F	2.80E-02	2.80E-02	2.80E-02	2.80E-02	No	No	No	N
4		F	2.33E-03	2.33E-03	2.33E-03	2.33E-03	No	No	No	N
5		F	1.14E-02	1.14E-02	1.14E-02	1.14E-02	No	No	No	N
6		F	2.53E-03	2.53E-03	2.53E-03	2.53E-03	No	No	No	N

Setup Type	Setup ID	Run	Result
MCS Analysis Specification	DEFAULT	Yes	Yes
Uncertainty Analysis Specification	DEFAULT	Yes	Yes
Importance Analysis Specification	DEFAULT	Yes	Yes
Time-dep. Analysis Specification	DEFAULT	Yes	Yes

Analysis Sequence BC Set Memos

IS Требование на останов

Рис. 2.8.6. Результаты расчета вероятности реализации аварийных последовательностей с учетом вероятности поступления требования на останов объекта

RiskSpectrum PSA Professional - C:\RISKSPEC\ERSHOV\ZASHITA.RSD - [Consequence Analysis Case(1):OK]

File Edit Record View Analysis Tools Window Help

ID - Char. # 1	Description	Calc.type	Mean	5th perc.	Median	95th perc.	Text Result	Gate Out	BE Out	Exch
CD		F	4.86E-03	5.05E-03	5.05E-03	5.05E-03	No	No	No	N
OK		F	1.81E-01	1.81E-01	1.81E-01	1.81E-01	No	No	No	N
OK1		F	3.29E-02	3.29E-02	3.29E-02	3.29E-02	No	No	No	N

Setup Type	Setup ID	Run	Result
MCS Analysis Specification	DEFAULT	Yes	Yes
Uncertainty Analysis Specification	DEFAULT	Yes	Yes
Importance Analysis Specification	DEFAULT	Yes	Yes
Time-dep. Analysis Specification	DEFAULT	Yes	Yes

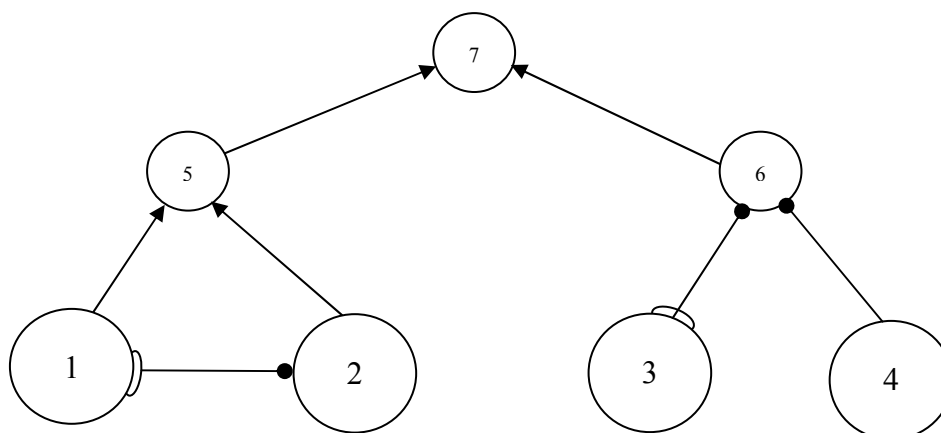
Analysis Consequence Event Tree BC Set Memos

Рис.2.8.7. Результаты расчета вероятностей реализации отдельных конечных состояний системы с защитой при аварии

Как следует из результатов расчета, в ряде случаев получено довольно хорошее схождение с результатами расчетов с помощью ПК Relex. Однако в большинстве случаев результаты расчета вероятности аварии не совпадают с результатами расчетов по ПК Relex. Как отмечалось в п. 2.8.3, не совпали результаты расчетов по ПК Relex и с результатами, полученными с помощью ПК АСМ СЗМА.

Для выяснения причин данного расхождения задача была решена с помощью ПК NEWАСМ. СФЦ, отображающая моделируемую ситуацию, представлена на рис. 2.8.5. Здесь вершина №1 отображает случайное событие работоспособности системы защиты на момент поступления требования на остановку объекта. Вероятность этого события в соответствии с принятыми исходными данными, составляет 0.923116347. Вершина №4 отображает случайное событие работоспособности системы защиты в момент выполнения требования на остановку объекта. Вероятность данного события принята равной вероятности события №1. События №2 и №3 представляют собой случайные события работоспособности объекта.

Все события в СФЦ – **неразмноженные**. Такое решение принято в результате детального анализа данных, представленных на рис.2.8.2. Ручные расчеты вероятности реализации отдельных ветвей дерева показывают, что, например, работоспособность системы защиты представлена на нем тремя случайными событиями, имеющими вероятность отказа (слева направо) – 0.0376552, 0.039198 и 0.076884.



В таблице 2.8.3.б представлены сводные результаты расчетов вероятности реализации отдельных аварийных ситуаций с помощью всех четырех кодов.

Таблица 2.8.3.б.

№№ п/п	Описание логического критерия	Результаты расчетов			
		Relex	NEWАСМ	Risk Spectrum	Технология АСМ
1	Авария	0.00682572	0.0048396	0.004858	0.006829062
2	«Первый» штатный останов	0.00710542	-		0.00710758
3	«Второй» штатный останов	0.167333	0.167332553	0.1545	0.167332605
4	Авария + первый штатный останов	0.013882605	0.013936647		
5	Вершинное событие	0.178892	0.17893714531	0.18131	0.181269247

Как следует из представленных данных, расчеты по различным кодам практически нигде не совпадают. Причина расхождения для кодов NEWАСМ и АСМ СЗМА – использование размноженных вершин во втором случае. При использовании размноженных вершин в СФЦ рис.2.8.3 имеем практически полное совпадение результатов расчета.

Причины расхождения с результатами кода Relex требуют изучения.

Сводная таблица результатов раздела 2.8. " Расчет надежности системы с защитой "				
Параметры элементов	Характеристики задачи	Результаты моделирования и расчетов		
		Relex Fault Tree	ПК АСМ	Risk Spectrum
1	2	3	4	5
интенсивность отказов устройства контроля = $3e-6$;	Аварийный отказ объекта	0.00682572	0.0068290623	0.004858
	Первый штатный останов	0.00710542	0.0071075797	не вычислена
интенсивность отказов исполнительного устройства = $5e-6$;	Второй штатный останов	0.167333	0.1673326049	0.1545
	Общая вероятность двух штатных остановов		0.1744401847	
интенсивность отказов Объекта = $2e-5$;	Отказ объекта	0.178892	0.181269	0.18131

ВЫВОДЫ ПО РАЗДЕЛУ 2.8

Выводы специалистов ИПУ РАН

В разделе рассматривается простейшая задача, для моделирования которой требуется учесть последовательность возникновения отказов. Подобные задачи встречаются практически всегда, когда рассматривается контроль и реакция на него. Задача правильно решена на ПК Relex и ПК АСМ. Предложенные решения на ПК Risk Spectrum неверны. Используемая в ПК Risk Spectrum логико-вероятностная технология принципиально не позволяет решать задачи данного класса (т.е. учитывать последовательность возникновения отказов). Незначительные расхождения решений на ПК Relex и ПК АСМ объясняются тем, что мы решали задачу «по умолчанию», когда устанавливается точность 10^{-3} . При установке нами точности 10^{-6} (а максимально возможная – 10^{-8}) шесть цифр решений на ПК Relex и ПК АСМ совпали.

Отметим, что учет возможности несовместных видов отказов и последовательности их возникновения является специфической особенностью систем с защитой и, в общем случае, – анализа опасностей, безопасности.

Выводы специалистов ОАО "СПИК СЗМА"

1. Непосредственно в программных комплексах АСМ средства решения задач данного класса еще не внедрены. Теоретическая и программная разработка метода учета последовательностей отказов в технологии АСМ завершена. Получено общее аналитическое решение задачи расчета вероятности любой последовательности отказов элементов системы отдельно и в совокупности с группой элементов, проработавших безотказно (для случая экспоненциального закона распределения времени их безотказной работы). Для проведения НИР использовалась программная утилита АСМ-последовательности, в которой реализован разработанный метод вычислений вероятностей заданных последовательностей отказов элементов, которая в настоящее время внедряется в ПК АСМ СЗМА.
2. Все расчеты вероятностей промежуточных событий данного примера (аварийный отказ, первый штатный и второй штатный отказы), полученные с помощью утилиты АСМ, практически совпали с результатами соответствующих расчетов, полученных с помощью модуля Relex Fault Tree (см. первые три строки сводной таблицы раздела 2.8). Отличия начинаются только в пятом-шестом разряде. По нашему опыту даже такие, незначительные, на первый взгляд, отклонения необходимо

анализировать, поскольку в равноценных аналитических методах их не должно быть. Нам неизвестны методы решения, реализованные в модуле Relex Fault Tree, поэтому ответ на данный вопрос могут дать только дальнейшие совместные исследования.

3. Различия в расчете вероятности конечного результата более существенные. Расчеты утилитой АСМ-последовательности дают общую вероятность отказа объекта **0.181269**, а результат модуля Relex Fault Tree составляет **0.178892**. Следует отметить, что простая сумма первых трех вероятностей, полученных Relex Fault Tree (см. сводную таблицу) дает результат **0.18126414**, который существенно ближе к результату, полученному с помощью утилиты АСМ. Уяснение причин такого расхождения нуждается в дополнительных исследованиях совместно со специалистами ИПУ РАН.

Выводы специалистов СПБАЭП

1. Задача решена всеми тремя программными комплексами, однако, результаты решения по различным критериям в большинстве случаев не совпадают. Не удалось установить и степень близости решений между отдельными кодами. В ряде случаев имеем большую близость решений между АСМ и Relex, в других – между АСМ и Risk Spectrum, в третьих – между Relex и Risk Spectrum.

2. Анализ научно-технической литературы по данному вопросу (Э. Дж. Хенли, Х. Кумамото. Надежность технических систем и оценка риска, М.: Машиностроение, 1984. стр. 58-60) показывает, что логический оператор «приоритетно И» может быть заменен комбинацию логических операторов «И». Следовательно, и код АСМ и код Risk Spectrum теоретически должны решать задачи указанного класса.

3. Необходимо продолжить исследования задач данного класса.