Особенности программной реализации методов количественного анализа риска аварий ОПО на основе логико-вероятностного моделирования

НОЗИК А.А.
Генеральный директор
АО «СПИК СЗМА», к.т.н.
alexander_nozik@szma.com
СТРУКОВ А.В.
Ведущий специалист исследовательского отдела, к.т.н. alexander_strukov@szma.com
МОЖАЕВА И.А.
Старший инженер-программист, к.т.н.
irina_mozhaeva@szma.com
АО «Специализированная инжиниринговая компания «Севзапмонтажавтоматика»,
+7 (812) 610-78-80, 199106, Санкт-Петербург, 26-я линия В.О., 15, корп. 2, лит. А,
Бизнес-центр «Биржа»

Приказом Ростехнадзора № 144 от 11.04.2016 утверждено Руководство по безопасности «Методические основы по проведению анализа опасностей и оценки риска аварий на ОПО» (далее Руководство) [1], которое устанавливает методические принципы, термины и определения в области анализа опасностей и оценки риска аварий на ОПО, а также представляет основные методы анализа риска.

В Руководстве отмечено, что при анализе опасностей, связанных с отказами технических устройств, АСУТП, систем противоаварийной защиты (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. При этом одной из оцениваемых характеристик опасности аварии является технический риск как вероятность отказа технических устройств с последствиями определенного уровня (ущерба). В этом случае говорят об опасном состоянии и вероятности наступления опасного отказа.

Существуют два основных подхода к оценке риска аварии:

- развитие модели надежности системы в сторону учета возможных инициирующих событий и условий (ИС и ИУ). При этом обычно структурная модель объекта не меняется, а в исходных данных общая интенсивность отказов элементов меняется на интенсивность опасных отказов;

- разработка самостоятельной модели безопасности, которая учитывает возможные отказы техники и персонала, варианты развития опасной (аварийной) ситуации, влияние внешних факторов.

Рассмотрим первый подход, предполагая, что интенсивность опасных отказов определяется также отказами по общим причинам (ООП).

Методология анализа риска с учетом ООП

Одной из задач анализа надежности систем безопасности ОПО является, в частности, анализ отказов по общей причине. В стандарте ГОСТ Р МЭК 61508-4-2007 (п. 3.6.10) дано следующее определение: Отказ **общего порядка (общей причины)** *(Common cause failure – CCF)* – отказ, который является результатом одного или нескольких событий, приводящих к **одновременному отказу двух или более отдельных каналов в многоканальной системе, приводящему к отказу системы в целом [2].**

Задачами анализа являются определение системных показателей (вероятность перехода системы в опасное состояние), а также оценка значимости как отдельных элементов, так и их сочетаний (в терминологии деревьев неисправностей – минимальных сечений отказов).

Для примера рассмотрим некоторую систему из четырех элементов X1, X2, X3 и X4, отказ которой определяется минимальными сечениями отказов элементов X1, X2, X3 и X4. В группу ООП входят три элемента (X1, X2 и X3), отказ четвертого элемента X4 является независимым [3].

Обозначим логическими переменными X_1, X_2, X_3 и X_4 события, реализация которых приводит к независимым отказам элементов X1¸X4. Логическими переменными CCF{X1,X2}, CCF{X1,X3}, CCF{X2,X3} и CCF{X1,X2,X3} обозначим события, связанные с одновременными отказами соответствующих элементов.

Логические условия отказа исследуемой системы *Ys* без учета ООП выражаются следующей булевой функцией, которая представляет собой логическую сумму (дизъюнкцию) минимальных сечений отказов (МСО) – конъюнкций:

$$Ys = X_1X_2 \vee \overline{X_1}X_2X_4 \vee X_1\overline{X_2}X_3X_4, \quad (1)$$

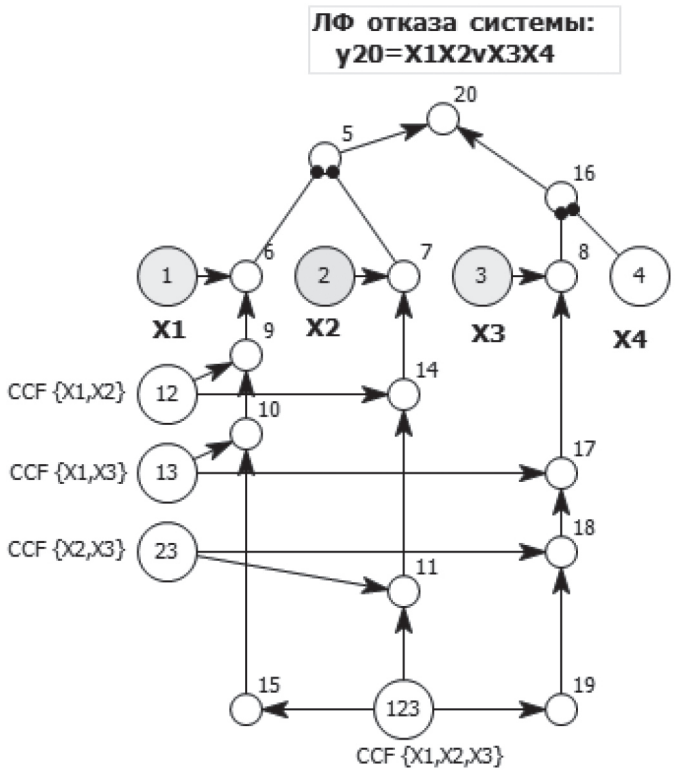
В рамках логико-вероятностного подхода для количественной оценки системных показателей и анализа значимостей отдельных элементов и МСО логическая функция (1) должна быть преобразована к виду, позволяющему корректно использовать основные теоремы теории вероятностей – о вероятности произведения независимых событий и вероятности суммы несовместных событий. На основе теоремы де Моргана и представления дизъюнкции $A \vee B$ в эквивалентной форме $A \vee \overline{A}B$ логическая функция (1) преобразуется в функцию вида

$$Ys = X_1X_2 \vee \overline{X_1}X_2X_4 \vee X_1\overline{X_2}X_3X_4, \quad (2)$$

в которой логические переменные заменяются на вероятностные характеристики событий, а логические действия – на алгебраические. Результатом логико-вероятностного преобразования является выражение для оценки вероятности отказа Q_s системы:

$$\Pr\{Ys=1\} = Qs = Q_1Q_2 + (1-Q_1)Q_3Q_4 + Q_1(1-Q_2)Q_3Q_4 \quad (3)$$

где Pr{*Ys*=1}=*Qs* вероятность истинности реализации логического критерия отказа исследуемой системы, то есть вероятность отказа системы;



Yc= y20

Логическая функция содержит 9 конъюнкций

№ кон.	ЛФ
1	CCF {X1,X2,X3}
2	CCF {X1,X2}
3	X3 X4
4	X4 CCF {X1,X3}
5	X4 CCF {X2,X3}
6	X1 CCF {X2,X3}
7	CCF {X1,X3} CCF {X2,X3}
8	X1 X2
9	X2 CCF {X1,X3}

Рис. 1. СФЦ и ЛФ отказа системы из 4 элементов с группой ООП

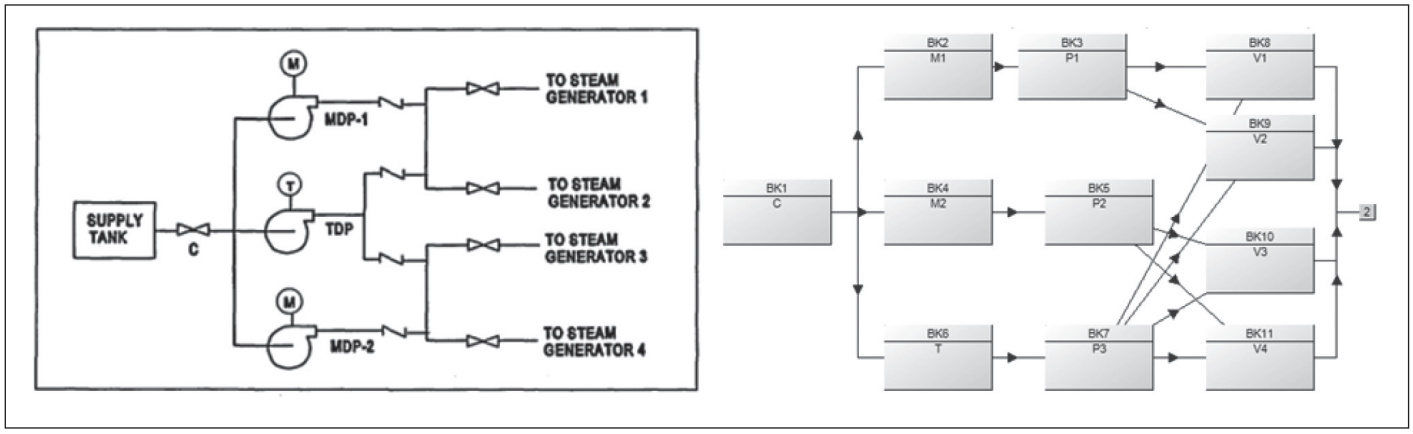


Рис. 2. Структурная схема и блок-схема надежности в программной среде Reliability Workbench вспомогательной системы подачи питательной воды

Pr{X_i=1}=Q_i – – вероятность истинности реализации события отказа *i*-го элемента, при этом Pr{$\overline{X}_i$=1}=1-Q_i

Значимость ξ_i (важность) *i*-го элемента определяется на основе частной производной

$$\xi_i = \frac{\partial Qs}{\partial Q_i}$$

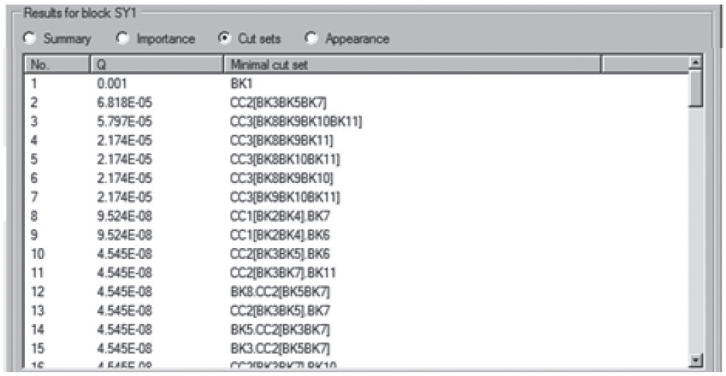
и соответствующего логико-вероятностного преобразования. Для исследуемой системы для случая равнонадежных элементов значимости элементов равны и вычисляются по формуле

$$\xi_i = Q_i - Q_i^3 , \quad (4)$$

Одним из способов введения ООП в модель надежности (безопасности) системы является явное отображение таких событий непосредственно на дереве отказов аналогично независимым отказам. На рис. 1 показана графическая иллюстрация этого способа на примере решения ранее сформулированной задачи структурным способом с использованием схемы функциональной целостности (СФЦ) в программной среде ПК АРБИТР [4].

На рис. 1 функциональные вершины СФЦ, соответствующие событиям независимых отказов элементов 1, 2 и 3, входящим в группу ООП, выделены серым цветом. Функциональные вершины 12, 13, 23 и 123 соответствуют логическим переменным CCF{X1, X2}, CCF{X1, X3}, CCF{X2, X3} и CCF{X1, X2, X3}. Условия отказа элемента X1 (фиктивная вершина 6) есть логическая сумма событий X1 (независимый отказ элемента 1) и событий CCF{X1, X2}, CCF{X1, X3} и CCF{X1, X2, X3}, то есть

$$y6 = X_1 \vee CCF\{X_1, X_2\} \vee CCF\{X_1, X_3\} \vee CCF\{X_1, X_2, X_3\} \quad (5)$$



а)

Логическая ФРС содержит 129/129 конъюнкций

№ кон.	Ркон.	Знач.кон	Сумм.знач.	ФРС
1	1.0000E-003	8.2388E-001	8.2388E-001	X1
2	6.8182E-005	5.6174E-002	8.8000E-001	CCF2[X3,X5,X7]
3	5.7971E-005	4.7761E-002	9.2771E-001	CCF3[X8,X9,X10,X11]
4	2.1739E-005	1.7910E-002	9.4560E-001	CCF3[X9,X10,X11]
5	2.1739E-005	1.7910E-002	9.6349E-001	CCF3[X8,X9,X11]
6	2.1739E-005	1.7910E-002	9.8137E-001	CCF3[X8,X9,X10]
7	2.1739E-005	1.7910E-002	9.9926E-001	CCF3[X8,X10,X11]
8	9.5238E-008	7.8465E-005	9.9934E-001	X6 CCF1[X2,X4]
9	8.0087E-008	6.5982E-005	9.9941E-001	CCF1[X2,X4] X7
10	4.5455E-008	3.7449E-005	9.9945E-001	X6 CCF2[X3,X5]
11	4.1126E-008	3.3882E-005	9.9948E-001	X4 CCF2[X3,X7]
12	4.1126E-008	3.3882E-005	9.9951E-001	X2 CCF2[X5,X7]
13	3.8223E-008	3.1491E-005	9.9954E-001	X3 CCF2[X5,X7]
14	3.8223E-008	3.1491E-005	9.9958E-001	X5 CCF2[X3,X7]
15	3.8223E-008	3.1491E-005	9.9961E-001	CCF2[X3,X5] X7
16	3.5903E-008	2.9579E-005	9.9964E-001	CCF2[X5,X7] X8

б)

Рис. 3. Фрагменты экранных интерфейсов вывода результатов анализа МСО в программных средах Reliability Workbench (а) и ПК АРБИТР (б)

Аналогично условия отказа для элементов X2 и X3 (фиктивные вершины 7 и 8 соответственно) запишутся в виде:

$$y7 = X_2 \vee CCF\{X_1, X_2\} \vee CCF\{X_2, X_3\} \vee CCF\{X_1, X_2, X_3\}, \quad (6)$$

$$y8 = X_3 \vee CCF\{X_1, X_3\} \vee CCF\{X_2, X_3\} \vee CCF\{X_1, X_2, X_3\}, \quad (7)$$

Логическая функция (ЛФ), описывающая условия отказа исследуемой системы $Y_{s\ OOП}$ с учетом ООП, то есть преобразования условия (1) на основе (5-7), показана в правой части рис. 1 как часть экранного интерфейса ПК АРБИТР.

Событие CCF{X1, X3)×CCF{X2, X3), приведенное в строке 7 ЛФ рис. 1, в зависимости от конкретных условий может трактоваться как конъюнкция (произведение) несовместных событий или исключаться из расчетов ввиду незначительного влияния на конечный результат [3]. Даже в случае исключения такого события формула ортогональной ЛФ после сокращений и упрощений выглядит намного сложнее формулы (2) (см. формулу 8).

Для ручного счета возможно использование формул аппроксимации, например, аппроксимации «ранних отказов» [3], при которой в предположении малой величины отказов высоконадежного оборудования вероятность отказа системы вычисляется как простая сумма вероятностей реализации конъюнкций ЛФ.

Современная программная реализации методов оценки риска аварий с учетом ООП предполагает автоматическое виртуальное построение расширенного дерева отказов без изменения графического изображения стандартного дерева отказов. Такой подход значительно упрощает процедуру анализа риска, размерность которой значительно увеличивается при учете ООП.

В качестве примера рассмотрим задачу анализа надежности вспомогательной системы подачи питательной воды [3, с.79], структурная схема которой показана в левой части рис. 2. В правой части рис. 2 приведена структурная схема надежности (RBD) в программной среде «Reliability Workbench™ from Isograph Ltd» [5].

Вспомогательная система подачи питательной воды состоит из двух идентичных насосов с электрическим приводом (M1P1, M2P2) и насоса с турбинным приводом (TP3). Система выполняет свои функции, если питательная вода из емкости T поступает в парогенератор хотя бы через два клапана V1¸V4.

В соответствии с методикой количественного анализа риска [3] после идентификации элементов, образующих группы ООП, осуществляется включение базовых событий ООП в дерево отказов системы и разработка их параметрического представления. В данном примере естественным образом формируются три группы элементов с ООП: группа электрических приводов M1 и M2, группа насосов P1-P3 и группа клапанов V1¸V4. Следующим шагом количественного анализа риска является формирование минимальных сечений отказов (МСО) без учета и с учетом ООП.

Число и состав МСО зависят от принятия гипотезы о совместности событий, входящих в одну группу ООП. Как отмечалось выше, вопрос о совместности таких событий является дискуссионным и трактуется в зависимости от конкретных условий задачи. Для данного примера в случае принятия гипотезы о совместности событий, входящих в одну группу ООП, число МСО составляет 129. В случае принятия гипотезы о несовместности таких событий число МСО составляет 114 [NUREG].

На рис. 3 представлены фрагменты экранных интерфейсов отчетов программных комплексов Reliability Workbench и ПК АРБИТР с отображением части таблиц результатов с МСО.

На рис. 3б показан фрагмент отчета ПК АРБИТР для случая принятия гипотезы о совместности событий, входящих в одну группу ООП. Логическая функция в этом случае содержит 128 конъюнкций (МСО).

На рис. 3а показан фрагмент отчета Reliability Workbench для случая принятия гипотезы о несовместности событий, входящих в одну группу ООП. Кроме того, алгоритм, реализованный в программе Reliability Workbench, события типа «CCF [X1, X2] CCF[X3, X4]» представляет в виде события «CCF [X1, X2, X3, X4]». Тогда число МСО сокращается со 114 до 111. Принятие такой же гипотезы в алгоритме ПК АРБИТР приводит к получению тех же 111 МСО. Эта процедура соответствует рекомендациям по исключению дополнительных МСО при проведении вероятностного анализа безопасности АЭС [6].

В таблице представлены результаты

$$\begin{aligned}
Ys_{OOП} = {} & CCF\{X_1, X_2\} \vee \overline{CCF\{X_1, X_2\}}\, CCF\{X_1X_2X_3\} \vee \overline{CCF\{X_1, X_2\}}\, \overline{CCF\{X_1, X_2, X_3\}}\, X_1X_2 \vee \\
& \vee \overline{CCF\{X_1, X_2\}}\, \overline{CCF\{X_1, X_2, X_3\}}\, (\overline{X_1} \vee X_1, \overline{X_2})\, X_3X_4 \vee \\
& \vee \overline{CCF\{X_1, X_2\}}\, \overline{CCF\{X_1, X_2, X_3\}}\, \overline{X_2}\, \overline{X_3X_4} X_1 CCF\{X_2, X_3\} \vee \\
& \vee \overline{CCF\{X_1, X_2\}}\, \overline{CCF\{X_1, X_2, X_3\}}\, \overline{X_1}\, \overline{X_3X_4}\, X_2\, CCF\{X_1, X_3\} \vee \\
& \vee \overline{CCF\{X_1, X_2\}}\, \overline{CCF\{X_1, X_2, X_3\}}\, \overline{X_2}\, \overline{X_3} (\overline{X_1} \vee X_1 \overline{CCF\{X_1, X_3\}})\, X_4 CCF\{X_1, X_3\} \vee \\
& \vee \overline{CCF\{X_1, X_2\}}\, \overline{CCF\{X_1, X_2, X_3\}}\, \overline{X_1}\, \overline{X_3}\, \overline{CCF\{X_1, X_3\}}\, X_4 CCF\{X_2, X_3\}.
\end{aligned}$$

Формула 8

Таблица. Результаты оценки вероятности отказа вспомогательной системы подачи питательной воды

Программная среда	Число МСО	Qs
ППК АРБИТР, Reliability Workbench	29	0.00100028
ПК АРБИТР	129	0.00121377
ПК АРБИТР	111	0.00121385
Reliability Workbench (Esary-Proshan)	111	0.00121392
Reliability Workbench (Rare)	111	0.00121415

оценки вероятности отказа вспомогательной системы подачи питательной воды Qs различными программными алгоритмами. Предполагалось, что вероятности отказов всех элементов системы равны q=0.001.

В таблице значения Qs в ПК АРБИТР получены точными методами, в Reliability Workbench – приближенными методами, указанными в скобках. Результаты таблицы показывают, что учет групп элементов с ООП заметно увеличивает вероятность отказа резервированной системы. Принятие гипотез о совместности событий в группах с ООП, а также использование точного или приближенных методов расчета незначительно влияют на конечный результат.

При использовании алгоритмов автоматического учета ООП следует внимательно относиться к тем допущениям и предположениям, которые легли в основу предлагаемого метода. Точный учет специфики конкретной задачи анализа риска может быть реализован только с использованием явного отображения всех событий и причин непосредственно на дереве. Использование упрощенных методов, как справедливо указано в [6], допустимо только для очень простых по структуре систем и небольшого числа элементов.

Кроме того, следует учитывать и особенности состава исходной информации об отказах элементов. Существуют два способа ввода информации об ООП. Например, для модели b-фактора вероятность независимого отказа элемента Qi является частью общей вероятности отказа Q_T, то есть Qi=(1-b)Q_T. Тогда вероятность отказа по общей причине Q_{CCF} определяется как произведение Q_{CCF} = bQ_T. Такой способ задания исходных данных описывает тот случай, когда в статистике отказов присутствуют как независимые отказы, так и отказы по общей причине. Если имеется «чистая» статистика только независимых отказов, тогда принимается Qi=Q_T.

Покажем различия в задании исходных данных на простом примере. Пусть при построении дерева неисправностей для некоторого элемента a ввели следующие исходные данные: b=0.05 и Qa =0.01. Тогда в первом случае вероятность одиночного (независимого) отказа элемента a будет Qai =(1-b)×Qa=(1-0.05)×0.01=0.0095, а вероятность отказа по общей причине Qa_{CCF}=b×Qa=0.05×0.01=0.0005. Для второго случая Q_{CCF} =bQ_T=0.05×0.01=0.0005 и Qi = Q_T =0.01. Тогда для дублированной системы использование различных исходных данных (включающих или не включающих в себя статистику ООП) даст следующие результаты: вероятность отказа системы Qs рассчитывается по формуле Qs= Q_{CCF}+(1-Q_{CCF})Q_i^2.

В первом случае (статистика ООП включена в оценку вероятности отказа элементов) Qs=0.5995×10^{-3}, во втором случае (статистика ООП не включена в оценку вероятности отказа элементов) Qs=0.5902×10^{-3}.

При разработке алгоритмов оценки риска с учетом ООП также может быть использован подход, связанный с учетом принятия или непринятия гипотезы о несовместности событий, связанных с независимыми отказами и ООП. В одном случае общая вероятность отказа рассчитывается по формуле Q_T= Qi + Q_{CCF}, в другом Q_T= Qi + Qi – Qi× Qi. Гипотеза о совместности независимых отказов и отказов по общей причине носит чисто теоретический характер и может быть использована только при достаточном ее физическом обосновании [2].

Заключение

Необходимость учета ООП для анализа риска аварий ОПО в настоящее время предписывается нормативными документами МАГАТЭ и МЭК. В частности, многолетний опыт эксплуатации АСУ на объектах использования атомной энергии показал существенное влияние ООП на оценку надежности и безопасности резервированных устройств. Например, в стандартах серии МЭК 61508 при оценке соответствия аппаратных средств требуемым уровням безопасности (SIL) в расчетные формулы введена составляющая, учитывающая ООП.

Разработчики стандартов серии МЭК 61508 и МЭК 61511, соглашаясь с возможностью использования программных средств, разработанных для анализа надежности сложных систем, в задачах по анализу риска аварии призывают к более внимательному отношению к допущениям и упрощениям, принятым в тех или иных моделях, и корректному использованию исходных данных.

Очень важно, чтобы пользователь был компетентен в применении выбранного метода, и это, может быть, более важно, чем сам используемый метод. «Аналитик отвечает за то, чтобы гипотеза, лежащая в основе любого конкретного метода, была выполнена для рассматриваемого применения, либо была внесена какая-либо необходимая корректировка для достижения соответствующего реалистичного консервативного результата... Если для проведения расчетов используется программное обеспечение, то специалист, выполняющий расчет, должен понимать формулы/методы, используемые в программном пакете, чтобы быть уверенным в том, что они применимы в каждом конкретном случае» [2].

Одним из способов достижения этой цели является широкое обсуждение теории и практики анализа риска аварий на страницах научно-практических журналов.

Литература

1. РБ «Методические основы по проведению анализа опасностей и оценки.

2. ГОСТ Р МЭК 61508 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1-7. 2012.

3. Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485. US NRC, 1998.

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 is a software product from Isograph Ltd, www.isograph.com.

6. Швыряев Ю.В. и др. Вероятностный анализ безопасности атомных станций. Методика выполнения. – М.: ИАЭ им. Курчатова. – 1992, 266 с.