

## ЗАКЛЮЧЕНИЯ

### 1. Заключение специалистов ИПУ РАН

Отметим основные особенности трех программных комплексов анализа надежности и безопасности систем.

Программные комплексы компании "СПИК СЗМА" и "RISK SPECTRUM" компании "RELKON" реализуют один класс "надежностных" моделей оценки показателей систем – класс логико-вероятностного моделирования (под "надежностными" моделями подразумеваются как модели классической надежности, так и модели безопасности и технической эффективности, в частности, производительности, пропускной способности, риска). Этот класс моделей можно назвать классом статических моделей, так как они позволяют вычислять показатели надежности, безопасности и эффективности систем в момент времени  $t$ , в зависимости от возможных наборов работоспособных и неработоспособных состояний элементов системы в данный момент времени. Причем процессы функционирования, отказов, восстановления любого элемента системы не зависят от других элементов, поэтому не требуется анализ происходящих событий на интервале функционирования. Такими показателями являются:

- коэффициент готовности (простоя; стационарный, нестационарный) или, в общем случае, вероятность застать систему в момент времени  $t$  в выделенном классе состояний системы;
- параметр потока отказов (стационарный, нестационарный);
- средняя эффективность в момент времени  $t$ .

Для систем, в которых восстановление элементов не предусмотрено, нестационарный коэффициент готовности совпадает с вероятностью безотказной работы (ВБР) на интервале  $(0, t)$ , поэтому логико-вероятностные модели позволяют в этом случае вычислять ВБР. Для систем с восстанавливаемыми элементами возможно приближенное оценивание ВБР применением, напр., асимптотических результатов теории регенерирующих процессов. Но такая возможность имеется лишь в случае всех восстанавливаемых элементов и экспоненциальных распределений случайных величин, причем  $\mu_i \gg \lambda_i$  (где  $\mu_i$ ,  $\lambda_i$  – интенсивности восстановления, отказа элемента  $i$ ). Поэтому, напр., в примерах 3 (разделы 2.1.2-2.1.3), 2 (разделы 2.3.2-2.3.3), 2 (разделы 2.4.2-2.4.3) вычисленные оценки ВБР совпали. В случае смешанных систем (с восстанавливаемыми и невосстанавливаемыми элементами) или систем с неэкспоненциальными распределениями исходных данных (времен до отказа и восстановления) для элементов, когда среднее время восстановления не является величиной много меньшей средней наработки до отказа, получить оценку ВБР логико-вероятностными методами едва ли возможно. Может потребоваться решение дифференциальных или интегральных уравнений, или хотя бы реализация интегрирования функций от параметра потока отказов. Поэтому примеры 4 (раздел 2.1.2), и 4,6 (раздел 2.4.2) в части оценки ВБР решены лишь ПК "RELEX". Аналогично обстоит дело и со средними наработками (средними временами). Лишь для случаев всех восстанавливаемых элементов с экспоненциальными распределениями времени до отказа и времени восстановления каждого элемента и для систем с невосстанавливаемыми элементами и экспоненциальным распределением времени до отказа элементов, могут быть получены оценки средних времен логико-вероятностными методами без интегрирования различных выражений (см. п.п. 1.2.4.1.2 и 1.2.4.2.3). В общем случае потребуется реализация более сложных процедур расчета и оценки, которые и реализованы в ПК "RELEX".

В ПК "RELEX" реализованы как статические модели "надежностного" анализа систем (логико-вероятностное моделирование с логическими функциями И, ИЛИ, НЕ, К/Н как в

RELEX RBD, так и в RELEX Fault Tree), так и динамические модели во всех аналитических модулях (RELEX RBD, RELEX PBD, RELEX Fault Tree, RELEX MARKOV).

Программные комплексы компании "СПИК СЗМА" имеют исключительно удобный и наглядный аппарат задания моделей (СФЦ), объединяющий лучшие стороны технологий блок-схем надежности, графов связи, деревьев отказов, деревьев событий. Классическое логико-вероятностное моделирование дополнено учетом групп несовместных событий и процедурами оценки ВБР (для оговоренных выше случаев). Эти факторы (учет групп несовместных событий и возможности оценки ВБР) значительно расширяют область применения комплекса (по сравнению с классическим логико-вероятностным моделированием), особенно с точки зрения анализа опасностей (безопасности). В настоящее время проходит развитие программных комплексов компании "СПИК СЗМА" как раз для учета ряда динамических факторов (напр., последовательности возникновения отказов). Поэтому достаточно «мощное» и высококачественное логико-вероятностное моделирование дополняется методами марковского моделирования, другими методами оценки показателей надежности, безопасности.

Динамические модели позволяют принципиально учитывать любые факторы, зависимости и вычислять любые показатели. Другое дело, какие именно факторы учитываются при разработке программного продукта и какие методы оценки показателей реализовываются (в частности, в ПК "RELEX"). Практически все примеры в разделах 2.1.2, 2.2.2, 2.3.2, 2.4.2, 2.6.2, 2.8.2, 2.9.2, 2.10.2 демонстрируют, какие из особенностей систем реализованы с применением динамических моделей в ПК "RELEX". Перечислим как продемонстрированные в примерах основные особенности, зависимости систем, так и не вошедшие в примеры:

- учет произвольных распределений наработок до отказа и времени восстановления элементов;
- ненагруженное, облегченное, скользящее резервирование;
- фазы (этапы) работы элементов, блоков и системы в целом;
- учет несовместности отказов и последовательности их возникновения;
- учет временных задержек в срабатывании логических вершин (напр., некоторые виды временной избыточности);
- учет общих причин отказов не только в предлагаемых моделях ( $\alpha$ ,  $\beta$  факторные модели и т.п.), но и разработка собственных моделей на марковских процессах, с включением их в как в деревья, так и в блок-схемы;
- учет ограничений на число бригад по восстановлению и на ЗИП;
- учет возможности восстановления системы после её отказа и/или останова (когда в процессе функционирования восстановление недопустимо);
- реализация некоторых моделей контроля работоспособности (а не только модель с мгновенным проявлением и обнаружением отказа);
- учет технического обслуживания с возможностью восстановления не только работоспособности, но и ресурса (для элементов со "стареющими" распределениями).

**По мнению представителей ИПУ РАН при анализе и оценке показателей безопасности (опасности) недопустимо применение моделей, не учитывающих несовместные виды отказов элементов и системы в целом, последовательности возникновения отказов и методов, не позволяющих относительно аварийных состояний с различными последствиями, получать интервальные показатели типа вероятности возникновения**

**аварии вида  $i$  на интервале функционирования для систем с восстановлением элементов. Именно эти особенности и выделяют класс вероятностных моделей безопасности из всех моделей “надежностного” анализа.**

В ПК “RISK SPECTRUM” реализовано классическое логико-вероятностное моделирование (да ещё и приближенное, и основывающееся на представлении моделей только в виде деревьев). Решать на нём серьёзные задачи надежностного анализа сложных систем с особенностями невозможно (если иметь в виду адекватность моделирования). Самым крупным «промахом» разработчиков RISK SPECTRUM является то, что не вычисляются двухсторонние оценки по любой одной конструкции (минимальным сечениям, или минимальным путям) и по любому дереву как отказов, так и успехов не определяются и минимальные сечения и минимальные пути (хотя это легко реализуемо). Применение этого комплекса если и возможно, то только для достаточно простого анализа и на самых ранних стадиях проектирования.

Обсуждать заблуждения кого бы то ни было (пусть даже И.А.Рябина) в области марковского моделирования мы не будем. Без марковского моделирования, без статистического моделирования ни одна задача из области динамических моделей решена быть не может (напр., ненагруженный резерв, та же последовательность отказов и даже несовместность (задайте вопрос, откуда берутся эти вероятности несовместных отказов, если заданы законы распределения, да ещё неэкспоненциальные, да ещё с восстановлением)). Таких динамических задач вообще бесконечное множество в отличие от статических постановок и учитываемых в них факторов. Кое-что относительно марковского моделирования все же скажем. Возрастающая мощность вычислительной техники и автоматизация построения для некоторых случаев марковских моделей постепенно решают проблему размерности. Не только в RELEX реализованы эти методы (а то как же они решили целый ряд динамических задач, для которых мы не строили марковскую модель). Уже создан отечественный ПК УНИВЕРСАЛ основывающийся на марковском моделировании и позволяющий строить модели с десятком тысяч состояний (естественно не вручную). Помимо этого марковские модели можно «укрупнять», как точно (когда это возможно), так и приближенно (в противном случае). Алгоритмы эти разработаны, в том числе и нами. Применять такое моделирование надо не ко всей системе, а к отдельным частям, т.е. проводить декомпозицию, далее моделирование, далее агрегирование оценок показателей.

Представители ИПУ РАН предлагают, объединив усилия организаций, участвующих в данной работе, в течение нескольких ближайших лет провести разработку программного комплекса, содержащего как статические, так и динамические модели. Прекрасный аппарат задания моделей в виде СФЦ, объединяющий как блок-схемы (удобные для систем с явно выраженными функциональными структурами), так и деревья отказов/успехов, (удобные для анализа безопасности при отсутствии явно выраженных функциональных структур) необходимо дополнить динамическими моделями анализа и вычисления показателей. При желании можно сделать задание моделей и в виде блок-схем и в виде деревьев. Такая разработка будет соответствовать мировому уровню (а кое в чем и превосходить) и позволит не только в теоретическом плане быть “на уровне”, но и в практических разработках.

## 2. Заключение специалистов СПИК СЗМА

1. Мы считаем данное исследование актуальным и перспективным. Выражаем глубокую признательность коллегам за большой труд, предоставленные результаты, их глубокий и доброжелательный анализ. Это позволило обоснованно позиционировать созданные и используемые в Компании теорию, технологию и программные комплексы (ПК) автоматизированного структурно-логического моделирования (АСМ) в развитии данного научного направления в мире, осмыслить положительные и отрицательные стороны наших текущих результатов, скорректировать направления дальнейших работ, пути совершенствования и развития.
2. Результаты НИР подтвердили, что в области автоматизации процессов построения математических моделей надежности, безопасности и риска структурно сложных систем наибольшее практическое применение во всех трех рассмотренных технологиях нашли теоретические разработки, которые в отечественной науке получили наименование логико-вероятностных методов. Это высокое признание многолетнего труда основоположника и руководителя отечественной научной школы логико-вероятностного моделирования академика ИГОРЯ АЛЕКСЕЕВИЧА РЯБИНИНА [12, 13].
3. Выполненная разработка сводных таблиц сравнительных результатов для каждого из экспериментальных разделов 2.1- 2.12 данной НИР позволила сделать следующее обобщение:
  - во всех сводных таблицах приведены **179** показателей моделирования и расчета надежности, безопасности и риска систем, из которых **161** показатель (модели вычисления) определяется средствами технологии, реализованной в различных модулях ПК Relex Software;
  - **112** показателей получены с помощью программных модулей и утилит технологии АСМ;
  - из **112** показателей, определенных средствами технологии АСМ, значения **111** практически полностью совпали с результатами, полученными различными модулями ПК Relex;

Результат сравнительного анализа является, по нашему мнению, объективным подтверждением научной корректности теоретических основ и программных реализаций технологии и ПК АСМ, разработанных специалистами ОАО "СПИК СЗМА".

4. В настоящее время методы и средства технологии АСМ не позволяют автоматически строить ряд математических моделей и вычислять некоторые показатели, которые уже реализованы в технологиях Relex и Risk Spectrum (см. раздел 2.3 пример 2, раздел 2.4 пример 4, 6, 7, разделы 2.5 и 2.9). Для большинства указанных задач нами уточнены подходы, методы и средства их реализации в технологии и ПК АСМ. Работы по их внедрению осуществляются в Компании по перспективному и текущим планам разработки НТП.
5. Полученные в НИР результаты еще раз показали, что логическая полнота графических и аналитических (метод, алгоритм и программа "ЛОГ" [3, 4, 10, 11]) средств СФЦ обеспечивает реализацию в технологии и ПК АСМ всех возможностей основного аппарата моделирования – алгебры логики. Поэтому, средствами СФЦ в данной НИР были успешно представлены практически все типовые формы структурного описания систем – блок-схемы (см. рис.2.1.6, 2.2.6, 2.3.5, 2.4.4, 2.7.7, 2.8.3, 2.10.4, 2.12.2) деревья отказов (см. рис.2.7.8.а, 2.7.8.б, 2.7.14), деревья безопасности (см. рис.2.7.13), деревья событий (см. рис.2.11.1, 2.11.3) и комбинаторные звенья (см. рис.2.2.9, 2.2.10), и одна марковская модель (см. раздел 2.10, §2.10.3).
6. Разработка метода, алгоритма и программного модуля "ЛОГ" [10], являющегося (ядром) основой всех версий ПК АСМ [6, 8, 19 и др.], обеспечила возможность успеш-

ного решения (на единой методической основе АСМ) всех задач логического моделирования систем в данной НИР, и получения прямых и инверсных, монотонных и немонотонных логических ФРС. Именно логически универсальный (в базисе операций "И", "ИЛИ", "НЕ") графический аппарат СФЦ и соответствующий метод, алгоритм и программный модуль ЛОГ, являются главной положительной, основой и отличительной особенностью технологии и ПК АСМ, разрабатываемых в ОАО "СПИК СЗМА".

7. Результатами данной НИР практически подтверждена возможность средств СФЦ технологии АСМ реализовать как прямую (блок-схемы, графы связности и т.п.) так и обратную (деревья отказов, деревья событий) структурную постановку задач (см. §2.7.3 и §2.12.3). Выбор прямого или обратного подходов для решения практических задач предоставляется пользователю технологии и ПК АСМ. Этот выбор удобен в тех случаях, когда рассматриваемые системы имеют существенно различающиеся по размерности и сложности прямые или обратные структурные модели. Например, прямую СФЦ (см. рис.2.1.6) системы электроснабжения (см. рис.2.1.1) разработать значительно легче, чем построить эквивалентное ей дерево отказов (см. рис.2.1.10). Вместе с тем, технология АСМ позволяет средствами СФЦ осуществлять все виды и обратной постановки задач, т.е. представлять деревья отказов, деревья событий и их совместные комбинации (см. рис.2.7.8.а, 2.7.8.б, 2.7.13, 2.7.14 и др.).
8. В примере 8 §2.1.3, рассмотрена задача автоматического построения средствами технологии АСМ нового класса немонотонных логических и вероятностных моделей систем. Такие модели позволяют ставить и решать много важных специальных задач системного анализа надежности, безопасности и риска. Например, только с помощью немонотонных моделей возможен анализа систем "второго типа" (качественно-сложных), которые в разных несовместных состояниях характеризуются различными показателями эффективности или риска функционирования. Технология решения этого нового и перспективного класса задач в настоящее время реализована только в ОЛВМ и ПК АСМ.
9. В технологии АСМ приоритетными являются точные аналитические методы автоматизированного логического, вероятностного моделирования и расчетов показателей надежности и безопасности систем. Поэтому все логические модели систем, полученные в примерах программными средствами различных технологий (Relex, АСМ и Risk Spectrum) полностью совпали. Результаты аналитических расчетов показателей надежности и безопасности, полученные средствами Relex и АСМ, практически полностью совпали в 111 случаях из 112 сопоставимых вычислений.
10. Результаты решения примеров данной НИР показали, что различия точных расчетов показателей надежности и безопасности, полученные средствами Relex и АСМ, и приближенных расчетов, полученных средствами ПК Risk Spectrum, при вероятностях отказов элементов менее 0.01 ( $q_i \leq 0.01$ ) как правило, незначительные. При  $q_i > 0.01$  расхождения расчетов системных показателей могут быть существенными (см. табл.2.1.7, 2.1.15, 2.1.16). По нашему мнению, приближенные расчеты должны быть только вспомогательным средством анализа надежности и безопасности сложных систем в технологиях автоматизированного моделирования.
11. Кроме указанных существует большое количество других специальных направлений развития теории и технологии автоматизированного структурно-логического моделирования, над которыми сейчас работают специалисты ОАО "СПИК СЗМА". Эти направления во многом определяются объективными потребностями практики в адаптации данной технологии и ПК АСМ к решению задач автоматизированного моделирования и расчета показателей надежности и безопасности специальных системных объектов в различных отраслях промышленного производства. Одним из таких важных направлений является, по нашему мнению, разработка специализированных программных систем комплексного автоматизированного моделирования и оценки ожидаемого ущерба от возможных аварий на опасных производственных объектах. Главная особенность

этого направления заключается в эффективном объединении методов и средств автоматизированного моделирования и расчета вероятностных характеристик сценариев развития аварий с методами и средствами автоматизированного моделирования и расчета возможных последствий аварий на опасных производственных объектах [26].

### 3. Заключение специалистов СПБАЭП

1. В результате выполнения НИР получен ценный практический материал, позволяющий производить сравнительную оценку различных подходов к автоматизированному моделированию и расчету показателей надежности и безопасности сложных технических систем. Значимость и достоверность результатов работы во многом определена тем, что кроссверификация сравниваемых кодов производилась специалистами трех организаций, каждая из которых была заинтересована в отстаивании и защите своих методов. Это практически исключило возможность односторонних оценок, предвзятость оценок и т.п.

2. По существу все три сравниваемых программных комплекса используют одну и ту же методологию моделирования, подразумевающую поэтапное построение моделей надежности и безопасности разного вида:

- формализация модели с помощью графов того или иного вида;
- автоматическое преобразование графической модели в функцию алгебры логики;
- автоматическое преобразование логической функции в расчетный вероятностный многочлен (вероятностную функцию);
- производство расчетов требуемых показателей надежности и безопасности.

В то же время пути реализации данной технологии на практике отличаются, что во многом сказывается на адекватности получаемых результатов.

3. Код Risk Spectrum реализует практически классическую технологию формализованной постановки задачи моделирования с помощью деревьев событий и деревьев отказов. Нельзя не согласиться с мнением специалистов СПИК СЗМА о том, что данная технология имеет ряд недостатков. Как следует из результатов решения рассмотренных в НИР примеров, графические модели одних и тех же систем, представленные в виде деревьев отказов, значительно более громоздки, чем блок-схемы и СФЦ. Это вызывает и относительно большую трудоемкость их построения. Возможно, именно этим обстоятельством вызвано то, что в коде Relex для графического моделирования используются и деревья отказов и блок-схемы. В этой связи использование аппарата СФЦ, позволяющего моделировать как прямую, так и обратную логику рассуждений является более предпочтительным.

4. К сожалению, в коде Risk Spectrum не реализована возможность использования одной из базовых логических операций – операции отрицания, что снижает качество получаемых моделей. В двух других кодах эта возможность реализована, причем в коде Relex – при использовании деревьев отказов.

5. Все три кода позволяют автоматически получать по исходному графу логическую функцию неработоспособности системы. В то же время коды АСМ и Relex позволяют автоматически получать и логические функции работоспособности, что в ряде случаев является важным преимуществом.

6. Код АСМ обеспечивает преобразование логической функции в вероятностную функцию, представляемую в ортогональной дизъюнктивной нормальной форме, что исключает потерю точности при вероятностных расчетах. В коде Risk Spectrum для этих целей используются аппроксимирующие приближения, обеспечивающие получение только приближенных оценок показателей надежности и безопасности. При анализе надежности и безопасности систем, состоящих из высоконадежных элементов (вероятность отказа  $q_i \leq 0.001$ ), применение данного подхода, в принципе, допустимо, однако при использовании в составе систем оборудования с низкой надежностью расчеты с помощью Risk Spectrum дают завышенные (иногда чрезмерно завышенные) оценки вероятности отказа, что может приводить к принятию неверных проектных и иных решений.

Указанный недостаток кода Risk Spectrum особенно ярко проявляется при анализе надежности персонала, т.к. вероятности ошибок персонала, как правило, имеют высокие значения. В то же время, как известно, вклад ошибок персонала в ЧПЗ, особенно в стояночных

режимах, весьма высок (особенно для стояночных режимов: 96% - для Тяньваньской АЭС, около 100% - для 3-го блока Калининской АЭС).

Судя по результатам решения примеров, код Relex обеспечивает получение точных результатов расчетов, однако из материалов НИР, представленных специалистами ИПУ, не ясно, каким образом это достигается.

7. Специалисты СПИК СЗМА и СПБАЭП отрешали все примеры с помощью одной и той же (в зависимости от используемой в данной организации) технологии. Специалисты ИПУ РАН использовали целый ряд технологий. С одной стороны, это подчеркивает достоинства кода Relex, однако с другой стороны – не позволяет сравнить, например, достоинства и недостатки технологии ДС/ДО, реализованной в кодах Relex и Risk Spectrum. Учитывая, что при выполнении ВАБ объектов ядерной энергетики технология ДС/ДО является стандартом де-факто (особенно на Западе), это является определенным недостатком (в рамках данной НИР).

8. Как следует из результатов НИР, код Risk Spectrum обеспечивает возможность использования более сложных, чем традиционно применяемые, моделей надежности элементарных событий, например, моделей, учитывающих принятую на АЭС стратегию периодических проверок и восстановлений элементов, входящих в различные каналы систем безопасности. На наш взгляд это большее достоинство, чем возможность использования закона Вейбулла-Гнеденко и т.п., особенно, если учитывать всем известную проблему со сбором статистических данных по надежности оборудования. В атомной энергетике, где применяется высоконадежное и малосерийное оборудование, вряд ли когда-нибудь удастся корректно определять параметры масштаба и формы 2-параметрических законов распределения. А это ставит под сомнение ценность их использования при решении практических задач анализа надежности и безопасности АЭС.

9. Важным достоинством кода Risk Spectrum является, на наш взгляд, его ориентация на решение задач большой размерности. Известно, что модели безопасности таких сложных объектов, как АЭС включают огромное количество элементов (В модель безопасности АЭС «Бушер», например, входят 84 дерева событий, 984 дерева отказов, 2678 операторов, 3399 базовых событий, 73 функциональных событий, 205 групп ООП). Решение задач такой размерности, как известно, связано с целым рядом проблем. К сожалению, в данной НИР не ставилась задача сравнения кодов при анализе надежности и безопасности больших систем.

10. Судя по косвенным данным, ядро кода Risk Spectrum работает (фактически) в среде операционной системы MS DOC, что накладывает сильные ограничения на размерность моделей безопасности и приводит к грубым ошибкам расчета, связанным с отсечением, так называемых «малозначащих сечений». Код АСМ СЗМА лишен данного недостатка. Код NEWАСМ решает указанную задачу за счет корректного решения задачи полуавтоматической декомпозиции. Как решена данная задача в коде Relex, по результатам НИР определить не представляется возможным.