ГОСУДАРСТВЕННЫЙ КОМИТЕТ
ПО ИСПОЛЬЗОВАНИЮ
АТОМНОЙ ЭНЕРГИИ СССР

Атомная техника за рубежом

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ПЕРЕВОДНЫХ МАТЕРИАЛОВ
ИЗДАЕТСЯ С СЕНТЯБРЯ 1957

№ 3, март 990

УДК 621.039.58'68

УЧЕТ ЗАВИСИМЫХ ОТКАЗОВ ОБОРУДОВАНИЯ В ВЕРОЯТНОСТНЫХ АНАЛИЗАХ БЕЗОПАСНОСТИ АЭС

Токмачев Г. В.

Неидентифицированные зависимости между структурными элементами систем безопасности, случайное возникновение ненормальных условий окружающей среды, ошибки при проектировании, изготовлении, монтаже и пусконаладочных работах, а также неправильные действия оперативного и обслуживающего персонала могут привести к множественным отказам резервируемых элементов и, как следствие, к невыполнению одной или нескольких функций безопасности при авариях на АЭС. Признано, что зависимые отказы часто оказывают доминирующее воздействие на надежность систем безопасности. Например, анализ надежности системы аварийной подачи питательной воды в парогенераторы АЭС с реакторами PWR, независимо проведенный в нескольких странах [1—3], показал, что при учете зависимых отказов вероятность невыполнения функции этой системой увеличивается на несколько порядков по сравнению с результатами моделирования на основе учета только независимых отказов. Из результатов вероятностных анализов безопасности (ВАБ) шведских АЭС (табл. 1) следует, что зависимые отказы значимы для всех станций, и особенно для «Оскарсхамн-3» и «Форсмарк-3», оснащенных высокорезервированными четырехканальными системами безопасности.

Важность анализа зависимых отказов закреплена в нормативном документе МАГАТЭ [5], который предписывает предусматривать при проектировании меры, направленные против потери функций безопасности в результате повреждения по какой-либо общей причине нескольких элементов, систем или конструкций.

Однако отсутствие исходных данных и трудности моделирования зависимых отказов привели к тому, что ВАБ для нескольких АЭС проводились без их учета. Необходимость разработки методологии анализа зависимых отказов вызвала в последние годы осуществление ряда международных программ [1, 2, 6] и многочисленных исследований в различных странах как по созданию методики, так и по сбору и обработке исходных данных [3, 6—18].

Завершенные анализы зависимых отказов дают пока несогласующиеся между собой результаты, причинами чего являются использование противоречивых определений зависимых событий; недостатки используемых данных по зависимым событиям — отсутствие точных оценок их частоты влияния на систему, соотношения с частотой независимых событий, неприменимость к рассматриваемой системе — и, как следствие, их значительная неопределенность; ошибки или различные допущения при качественном и количественном моделировании зависимых событий [3,7, 8,19].

Таблица 1. **Вклад отказов по общей причине в вероятность плавления активной зоны [4]**

Энергоблок	Тип реактора	Год пуска	Вклад, %
«Оскарсхамн-1»	BWR	1972	20
«Оскарсхамн-3»	»	1985	75
«Барсебекк-1»	»	1975	19
«Рингхалс-1»	»	1976	44
«Рингхалс-2»	PWR	1975	15
«Форсмарк-3»	BWR	1985	90

Проблемы терминологии

В работах [1,11,20] отмечается отсутствие общепринятой терминологии в рассматриваемой области, в частности термины «зависимый отказ» и «отказ по общей причине» (или «отказ общего вида») иногда используются как синонимы. В то же время в работе [9] предпринята попытка дать основные определения:

зависимый отказ (dependent failure) — множественный отказ нескольких объектов, вероятность которого не может быть выражена просто как произведение безусловных вероятностей отказов индивидуальных объектов;

отказ по общей причине (common cause failure) — вид зависимого отказа, где одновременный (или почти одновременный) множественный отказ происходит по единичной причине; обычно сюда относят отказы, неявно моделируемые с помощью рассмотренных далее параметрических моделей;

каскадный отказ (cascade failure) — распространяющийся множественный отказ, когда отказ одного объекта является причиной отказа другого.

Эти термины используются в дальнейшем изложении.

Классификация зависимых отказов

Зависимость между различными объектами может быть вызвана или функциональными причинами, имеющими детерминистскую природу, или возникновением случайных событий стохастического характера [1]. Под функциональными причинами подразумеваются отказы других объектов (каскадные отказы), которые делятся на два типа: отказы, требующие ремонта данного объекта, и отказы, требующие только устранения их первопричины, т. е. восстановления объектов, отказавших первыми. В качестве объектов могут рассматриваться как отдельные элементы, так и целые системы безопасности или их каналы в случае отказа обеспечивающих, управляющих или смежных технологических систем (каналов). В общем случае условная вероятность отказа объекта при возникновении функциональной причины может отличаться от единицы, например, при рассмотрении отказа системы вентиляции в качестве функциональной причины.

Некоторые функциональные зависимости могут быть вызваны регламентными ограничениями, требованиями правил техники безопасности при проведении операций по техническому обслуживанию

или ремонту объектов. Возможны отказы объектов, вызванные исходным событием аварии.

Некоторые зависимые отказы обусловлены концептуальными проектно-конструкторскими ошибками, которые могут оказывать катастрофическое влияние на безопасность. К ним относятся невозможность или неэффективность выполнения функций безопасности в аварийных условиях системами, адекватно функционирующими при нормальной эксплуатации; функциональные зависимости, не выявленные при проектировании и нарушающие проектные требования; неадекватное проектирование средств диагностики и математического обеспечения ЭВМ, приводящее к реализации неверных алгоритмов управления оборудованием в аварийной ситуации средствами автоматики или персоналом [1, 7, 9].

Большую и разнородную группу зависимостей составляют ошибки, совершенные при реализации проектных решений [1, 8]. Это дефекты изготовления и монтажа оборудования, которые невозможно выявить имеющимися средствами в период заводских испытаний и пусконаладочных работ; дефекты, не выявленные из-за некачественных или проведенных в недостаточном объеме проверок в этот период; плохая настройка ободования из-за низкого качества пусконаладочных работ.

Ошибки при эксплуатации, приводящие к зависимым отказам, можно разбить на две группы [1, 8]:

неадекватное выполнение операций при техническом обслуживании и ремонте, приводящее к отказу каждой единицы оборудования с некоторой условной вероятностью, например, неточная настройка защиты, недозатяжка или перезатяжка шпилек, некачественное удаление вредной среды (воздух, вода, масло и др.);

выполнение ошибочных или невыполнение оперативных переключений в аварийной ситуации или в предшествующий ей период нормальной эксплуатации. Причиной этого являются низкая квалификация операторов, ошибочные действия персонала вопреки требованиям эксплуатационной документации и показаниям контрольно-измерительной аппаратуры. Такое игнорирование возможно из-за низкого качества документации или частых ложных показаний приборов.

Неблагоприятные условия окружающей среды, вызывающие множественные отказы [1, 5, 9, 11], можно разделить на две группы — внутренние и внешние по своему происхождению по отношению к АЭС. К первым относятся пожары, образование летящих предметов или водяных и воздушных струй при разрушении сосудов и трубопроводов под давлением или вращающихся механизмов, затопление или запаривание помещений, повышений в них температуры, взрывы, химическое, радиационное и вибрационное воздействие. Внешними воздействиями могут быть землетрясения, экстремальные погодные условия, падение самолета, разрушение плотины пруда-охладителя, воздействие живых организмов. Примером последнего фактора являются проблемы, возникшие с французскими дизель-генераторами [21]. В результате накопления воды на дне баков топлива произошло бурное размножение микроорганизмов, приведшее в течение 1—2 сут к изменению структуры дизельного топлива, засорению топливных фильтров и отказу дизель-генераторов.

Методы анализа зависимых отказов на качественном уровне

Идентификация и моделирование зависимых событий с самого начала должны быть включены в анализ надежности любой системы [1, 3, 8, 9, 12]. Исследование, не включающее анализ зависимостей, ведет к ошибочным результатам, особенно когда высокая безотказность достигается большой степенью резервирования. Поэтому анализ зависимых отказов проводится параллельно с анализом независимых отказов и включает те же этапы качественного и количественного анализа.

Цели качественного анализа — изучение механизмов и факторов, определяющих зависимости между элементами системы; идентификация потенциальных зависимых отказов, вызываемых другими элементами или системами (функциональные зависимости), которые должны моделироваться явно с помощью логических диаграмм (деревьев отказов или событий); идентификация групп элементов, которые могут быть подвержены общим воздействиям и должны моделироваться с помощью стохастических параметрических моделей; оценка эффективности предусмотренных средств защиты для предотвращения или ограничения масштабов зависимых отказов; классификация и просеивание идентифицированных потенциальных зависимостей; выбор для них адекватных моделей надежности [1, 7, 9].

На первом этапе качественного анализа система изучается. Для полноценного исследования необходима следующая информация по системе и входящему в нее оборудованию [2]: схемные решения, компоновка, функциональные связи, режимы эксплуатации, стратегия и объем технического обслуживания и проверок работоспособности, тип оборудования, отработанность его конструкции и физическая защищенность, завод-изготовитель, качество изготовления, монтажа, пусконаладочных работ и контроль за этим, квалификация обслуживающего персонала и защищенность оборудования от человеческих ошибок.

Методы качественного анализа можно грубо разделить на две группы [1]. В первой каждый вид отказа элемента анализируется по его влиянию и возможности распространения его причины на другие элементы или системы. Эти методы эффективны для идентификации функциональных зависимостей, которые могут моделироваться явно. Во второй группе методов анализ начинается с составления перечня причин, под воздействие которых могут попасть элементы рассматриваемой системы. Здесь необходимо уделить особое внимание факторам, влияющим на зависимость элементов системы [3]: использованию групп идентичных элементов, степени их функциональной и конструктивной разнопринципности, а также физического разделения, подверженности элементов различным нагрузкам из окружающей среды, по-

тенциальным человеческим ошибкам при проектировании, изготовлении, сооружении и эксплуатации, которые могут воздействовать на два и более элементов резервируемой группы.

Для анализа таких факторов удобен матричный метод [12]. Опыт показывает, что большинство отказов по общей причине происходило с идентичными активными элементами, которые первоначально эксплуатировались в одном режиме (ожидания или работы), причем виды отказов элементов были одинаковые.

В работах [3, 9] рекомендовано моделирование параметрических отказов по общей причине непосредственно на дереве отказов. Для каждого элемента на нем отображаются независимый отказ и каждая из воздействующих общих причин, которая встречается на дереве столько раз, на сколько элементов она влияет. Это увеличивает размеры дерева отказов в несколько раз.

Для упрощения дерева отказов возможно использование пороговых вероятностей отсечения ветвей дерева или предварительное просеивание всех идентифицированных зависимостей с целью включения в окончательную модель только важнейших эффектов. При этом можно применять простейшие количественные методы.

Для упрощения анализа во всех параметрических методах делается предположение о симметрии, т. е. зависимости вероятности любого события, вызванного общей причиной, только от числа отказавших элементов в результате возникновения этой причины [3].

В Великобритании в качестве альтернативного пути анализа отказов по общей причине принято введение их в модель после получения набора минимальных сечений на дереве, на котором моделируются только независимые отказы [12]. Для дальнейшего анализа зависимых отказов выбирают минимальные сечения, в которые входят два или более однотипных элементов или элементов, имеющих одинаковые признаки восприимчивости к воздействию какой-либо общей причины. При использовании такого метода существует опасность учета не всех минимальных сечений и переоценки некоторых из них [3].

Качественный анализ зависимых отказов вследствие различных воздействий окружающей среды предусматривает следующие этапы [1, 9]: составление перечня в максимальном объеме всех гипотетических внешних событий; мотивированное исключение из дальнейшего рассмотрения событий, которые не являются важными для места расположения данной системы (например, падение самолета, если отсутствуют их полеты; образование летящих предметов, если нет рядом вращающихся механизмов или сосудов под давлением и т. п.); определение зоны, на которой происходит данное воздействие; составление перечня элементов, расположенных в этой зоне; анализ степени защищенности элементов против данного воздействия.

Особое внимание должно уделяться анализу пожаров. Этот вид воздействия присущ всем без исключения АЭС, поэтому он должен обязательно учитываться при анализе зависимых отказов [5].

При проведении качественного анализа здания АЭС разбиваются на зоны, границами которых являются стены, пол, огнестойкие двери, кабельные проходки. В работе [22] принято, что уже через 25—30 мин произойдет отказ всех элементов в зоне и будет существовать условная вероятность распространения пожара в соседние зоны. Поэтому при анализе надежности пожарной сигнализации фактор времени имеет большое значение. Моделирование пожарной сигнализации и систем автоматического пожаротушения проводится с помощью обычных логических диаграмм. Рассматриваются также возможности применения переносных средств пожаротушения и воздействия воды и ее растворов на работоспособное электрооборудование.

Модели количественной оценки отказов по общей причине

Для количественной оценки отказов по общей причине, которые невозможно моделировать явно на дереве отказов, используют различные параметрические модели [1, 3, 7—18] — семейство методов β-фактора, модель основного параметра, биномиальную и полиномиальную модели интенсивностей отказов и др. В идеале параметрическая модель должна быть простой, универсальной, корректной, обеспечивать четкое определение параметров, совместимость с существующими источниками данных и возможность учесть специфичные для системы и ее элементов факторы, например, кратность резервирования [20]. Сложностью удовлетворения всей совокупности требований объясняется появление большого разнообразия параметрических моделей, в которых приоритет отдается тем или иным достоинствам.

Отметим разработанный в Великобритании экспертный метод отсечения [1]. В нормативных документах количественно оценены границы надежности системы в зависимости от степени ее резервирования и разнопринципности (см. рисунок). На основании качественного анализа этих факторов проводится усечение (сужение) интервала возможных значений вероятности отказа системы. Метод может быть полезен для предварительной оценки важности анализа отказов системы по общей причине.

Наиболее распространенной параметрической моделью является модель β-фактора [1—3, 7, 8, 10, 11]. Это объясняется простотой определения ее единственного параметра β (который требуется дополнительно к интенсивности отказов элементов системы), причем его оценки не зависят от наличия информации о числе требований на срабатывание системы или элементов. Численно β-фактор равен отношению интенсивности отказов элемента по общим причинам к полной интенсивности отказов элемента. Он позволяет определить интенсивность отказов по общим причинам группы λ_N, состоящей из любого числа N элементов, по формуле $\lambda_N=\beta\lambda_\Sigma$, где λ_Σ — полная интенсивность отказов одного элемента.

Диапазон изменения значений β довольно широк (0,03—0,24), что объясняется различными принципами отбора статистического материала для оценок. Часто встречаются высокие зна-

чения, близкие к 0,1, на получение которых влияет большое число общих элементов в резервируемых каналах систем безопасности зарубежных АЭС. Основной недостаток модели — излишний консерватизм при оценке глубоко резервируемых структур. В случае доминирующего влияния зависимых отказов модель дает одинаковые оценки показателей надежности двух-, трех- и четырехканальных систем.

Различные расширенные модели β-фактора разработаны для устранения этого недостатка [1—4,10]. В так называемой модели греческих букв введены три дополнительных параметра:

β—условная вероятность, что причина отказа одного элемента приведет к отказу еще, как минимум, одного элемента;

γ — условная вероятность, что общая причина отказа двух или более элементов приведет к отказу, как минимум, трех элементов;

δ—условная вероятность, что общая причина отказа трех или более элементов приведет к отказу не менее четырех элементов.

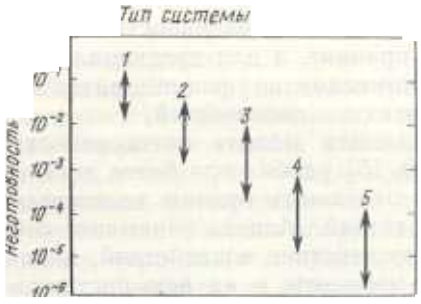
Если, например, рассматривается группа из четырех резервируемых элементов, то интенсивность отказов всех элементов этой группы по общей причине λ_4 определяется по формуле $\lambda_4=\delta\gamma\beta\lambda_\Sigma$. Если параметры γ и δ приравнять к единице, то получится рассмотренная модель β-фактора.

Основным недостатком модели греческих букв является трудность оценки параметров γ и δ, оказывающих решающее влияние на надежность системы. При оценках данных по дизель-генераторам, насосам и арматуре АЭС США диапазон изменения β составляет 0,08—0,18; γ — 0,5—0,94 (большая часть значений превышает 0,75); δ — 0,5—0,95 (большая часть значений превышает 0,9).

Подобные результаты получены при анализе статистики по клапанам с электроприводом на шведских АЭС. Эти оценки также имеют разброс в 2—2,5 раза из-за различных подходов к обработке эксплуатационных данных по отказам. Трудность при оценках параметров модели заключается в проблеме адекватного применения статистики по двухканальным системам при анализе систем с более высокой кратностью резервирования.

Процедура оценок параметров по эксплуатационной статистике для двух последних моделей несколько упрощается при использовании в них частот событий множественных отказов в системе вместо частот отказов элементов [9,13,14]. Модифицированные модели имеют аналогичные долевые коэффициенты и принципиально ничем не отличаются от предшественников. Это модели С-фактора (аналог β-фактора) и α-фактора (аналог модели греческих букв).

Существует [11,12] частичная модель β-фактора, имеющая некоторые сходные черты с экспертной моделью отсечения. Для однотипных резервируемых элементов задают начальное значение β-фактора 0,1—0,16 и диапазон изменения факторов, на него влияющих, например опыт персонала, проводящего техническое обслуживание, независимость проверки работоспособности элементов и др. Затем экспертно выбирают значения



Влияние структуры системы на ее надежность с учетом зависимых отказов: *1* — одноканальная система; *2* — резервированная система с однотипными каналами; *3* — резервированная система с каналами частично различного принципа действия; *4* — резервированная система с каналами совершенно различного принципа действия; *5* — две резервированные системы различного принципа действия

факторов в заданных диапазонах, которые складывают по законам логики, а полученное число используют для корректировки начального β-фактора. Для β-фактора установлены следующие нижние граничные значения: для резервируемой системы из однотипных элементов — 0,02, из разнотипных — 10^{-3}. Как утверждается в работе [11], надежность системы может быть улучшена резервированием не более чем в 50 раз и применением разнотипного резервируемого оборудования — еще в 20 раз.

Анализ причин зависимых и независимых отказов показывает [6], что они имеют различный отрицательный вклад в интенсивность этих двух категорий. Например, среди отказов по общей причине вызванные различными ошибками человека составляют 50 %, а среди независимых — 30 %. Поэтому высказано сомнение о возможности использования долевых коэффициентов β, γ, δ, полученных из других источников, при анализе системы, по которой имеются статистические данные о независимых отказах. Это, а также возможное завышение значений долевых коэффициентов вызвало предложения прямой оценки вероятностей (интенсивностей) отказов по общей причине [1, 3, 6, 9, 10], часто называемой моделью основного параметра. Согласно работе [6], где обработаны данные эксплуатационной статистики, различные элементы систем безопасности имеют при-

Таблица 2. **Интенсивность одновременного отказа двух одинаковых единиц оборудования по общей причине**

Наименование оборудования	
Исполнительные органы СУЗ	$2\cdot10^{-6}$
Дизель-генераторы	
Задвижки с электроприводом	
Предохранительные клапаны:	
отказ на открытие	$1\cdot10^{-6}$
отказ на закрытие	$3\cdot10^{-7}$
Насосы:	
отказ в режиме ожидания	$1\cdot10^{-}$
отказ в режиме работы	$6\cdot10^{-}$
Обратные клапаны:	
отказ на открытие	$7\cdot10^{-8}$
отказ на закрытие	$7\cdot10^{-8}$
Теплообменники	$5\cdot10^{-7}$
Вентиляторы	$7\cdot10^{-7}$

чения, близкие к 0,1, на получение которых влияет большое число общих элементов в резервируемых каналах систем безопасности зарубежных АЭС. Основной недостаток модели — излишний консерватизм при оценке глубоко резервируемых структур. В случае доминирующего влияния зависимых отказов модель дает одинаковые оценки показателей надежности двух-, трех- и четырехканальных систем.

Различные расширенные модели β-фактора разработаны для устранения этого недостатка [1—4,10]. В так называемой модели греческих букв введены три дополнительных параметра:

β—условная вероятность, что причина отказа одного элемента приведет к отказу еще, как минимум, одного элемента;

γ — условная вероятность, что общая причина отказа двух или более элементов приведет к отказу, как минимум, трех элементов;

δ—условная вероятность, что общая причина отказа трех или более элементов приведет к отказу не менее четырех элементов.

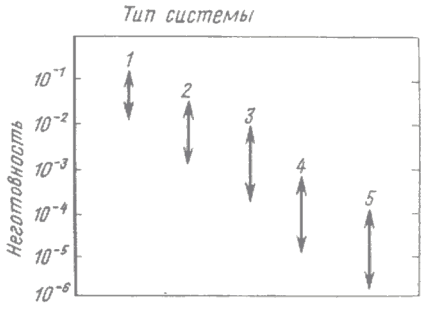
Если, например, рассматривается группа из четырех резервируемых элементов, то интенсивность отказов всех элементов этой группы по общей причине λ_4 определяется по формуле $\lambda_4=\delta\gamma\beta\lambda_\Sigma$. Если параметры γ и δ приравнять к единице, то получится рассмотренная модель β-фактора.

Основным недостатком модели греческих букв является трудность оценки параметров γ и δ, оказывающих решающее влияние на надежность системы. При оценках данных по дизель-генераторам, насосам и арматуре АЭС США диапазон изменения β составляет 0,08—0,18; γ — 0,5—0,94 (большая часть значений превышает 0,75); δ — 0,5—0,95 (большая часть значений превышает 0,9).

Подобные результаты получены при анализе статистики по клапанам с электроприводом на шведских АЭС. Эти оценки также имеют разброс в 2—2,5 раза из-за различных подходов к обработке эксплуатационных данных по отказам. Трудность при оценках параметров модели заключается в проблеме адекватного применения статистики по двухканальным системам при анализе систем с более высокой кратностью резервирования.

Процедура оценок параметров по эксплуатационной статистике для двух последних моделей несколько упрощается при использовании в них частот событий множественных отказов в системе вместо частот отказов элементов [9,13,14]. Модифицированные модели имеют аналогичные долевые коэффициенты и принципиально ничем не отличаются от предшественников. Это модели С-фактора (аналог β-фактора) и α-фактора (аналог модели греческих букв).

Существует [11,12] частичная модель β-фактора, имеющая некоторые сходные черты с экспертной моделью отсечения. Для однотипных резервируемых элементов задают начальное значение β-фактора 0,1—0,16 и диапазон изменения факторов, на него влияющих, например опыт персонала, проводящего техническое обслуживание, независимость проверки работоспособности элементов и др. Затем экспертно выбирают значения



Влияние структуры системы на ее надежность с учетом зависимых отказов: *1* — одноканальная система; *2* — резервированная система с однотипными каналами; *3* — резервированная система с каналами частично различного принципа действия; *4* — резервированная система с каналами совершенно различного принципа действия; *5* — две резервированные системы различного принципа действия

факторов в заданных диапазонах, которые складывают по законам логики, а полученное число используют для корректировки начального β-фактора. Для β-фактора установлены следующие нижние граничные значения: для резервируемой системы из однотипных элементов — 0,02, из разнотипных — 10^{-3}. Как утверждается в работе [11], надежность системы может быть улучшена резервированием не более чем в 50 раз и применением разнотипного резервируемого оборудования — еще в 20 раз.

Анализ причин зависимых и независимых отказов показывает [6], что они имеют различный отрицательный вклад в интенсивность этих двух категорий. Например, среди отказов по общей причине вызванные различными ошибками человека составляют 50 %, а среди независимых — 30 %. Поэтому высказано сомнение о возможности использования долевых коэффициентов β, γ, δ, полученных из других источников, при анализе системы, по которой имеются статистические данные о независимых отказах. Это, а также возможное завышение значений долевых коэффициентов вызвало предложения прямой оценки вероятностей (интенсивностей) отказов по общей причине [1, 3, 6, 9, 10], часто называемой моделью основного параметра. Согласно работе [6], где обработаны данные эксплуатационной статистики, различные элементы систем безопасности имеют при-

Таблица 2. **Интенсивность одновременного отказа двух одинаковых единиц оборудования по общей причине**

Наименование оборудования	
Исполнительные органы СУЗ	$2\cdot10^{-6}$
Дизель-генераторы	
Задвижки с электроприводом	
Предохранительные клапаны:	
отказ на открытие	$1\cdot10^{-6}$
отказ на закрытие	$3\cdot10^{-7}$
Насосы:	
отказ в режиме ожидания	$1\cdot10^{-}$
отказ в режиме работы	$6\cdot10^{-}$
Обратные клапаны:	
отказ на открытие	$7\cdot10^{-8}$
отказ на закрытие	$7\cdot10^{-8}$
Теплообменники	$5\cdot10^{-7}$
Вентиляторы	$7\cdot10^{-7}$

веденные в табл. 2 интенсивности парных отказов по общей причине, а для трехканальных и более систем рекомендовано использовать половинные значения этих интенсивностей.

Биномиальная модель интенсивности отказа [1—3, 9, 10, 15] удобна при более детальном рассмотрении отдельных причин зависимых отказов и их последствий. Модель описывает событие отказа как последствие воздействий, влияющих на отдельные элементы и на всю систему. Предполагается, что существуют два вида воздействий — нелетальные и летальные. При таком подходе интенсивность отказов по общей причине группы из четырех резервируемых элементов λ_4, например, определяется по формуле $\lambda_4=\mu p^4+\omega$, где μ и ω — интенсивность возникновения нелетальных и летальных воздействий соответственно; p — условная вероятность отказа элемента при нелетальном воздействии. Модель предполагает, что в случае возникновения нелетального воздействия отказы элементов являются условно независимыми и удовлетворяют биномиальному распределению, причем момент любого множественного отказа элементов синхронизирован. При летальных воздействиях все элементы отказывают с условной вероятностью 1. Общее число параметров биномиальной модели не зависит от кратности резервирования системы в отличие от моделей основного параметра и греческих букв, но превышает число параметров в этих моделях для двух- и трехканальных систем.

Интересны полученные на основании эксплуатационных данных США средние значения на требование показателей μ, ω и p соответственно: для насосов — $(6{,}55\div12{,}6)\,10^{-4}$, $(1{,}01\div2{,}67)\,10^{-3}$, $(2{,}51\div3{,}06)\,10^{-1}$; для арматуры с электроприводом — $1{,}37\cdot10^{-3}$, $5{,}1\cdot10^{-4}$, $2{,}93\cdot10^{-1}$; для обратных клапанов — $(1{,}84\div24{,}2)\,10^{-5}$, $(1{,}29\div16{,}9)\times\times10^{-3}$, $(4{,}8\div4{,}9)\,10^{-1}$.

К недостаткам модели относятся усложнение анализа при ее использовании и необходимость получения детализированной исходной информации, что не всегда реально. В частности, при оценке параметров модели по эксплуатационной статистике необходимо решать следующие проблемы [15]: выделение отказов по общей причине из всей совокупности множественных отказов, разделение последствий воздействий на летальные и нелетальные при полном отказе системы. Кроме того, эта модель очень чувствительна к различным предположениям [2].

Дальнейшее развитие и усложнение модели нашло отражение в работах [16—18], где предполагается, что параметр p биномиальной модели сам является случайной величиной с функцией распределения. В работе [16] исключено предположение о независимости отказов при нелетальных воздействиях. Поэтому введен дополнительный параметр, характеризующий меру защищенности системы от отказов по общей причине, например степень разнопринципности и физического разделения элементов. В работах [17, 18] вероятность отказа каждого элемента поставлена в соответствие определенной совокупности внешних факторов, переменных во времени. Несмотря на сложность установления такой зависимости, этот подход используется при подготовке окончательного анализа безопасности АЭС «Сайзуэлл-В» (Великобритания).

Полимиальная модель интенсивности отказов [10] является гибридом моделей греческих букв и биномиальной. Однако обилие параметров затрудняет ее использование и пока на практике эта модель еще не применялась.

Известны также модели общей нагрузки и множественных последовательных отказов [4]. В последней в качестве исходных данных требуется определение вероятности отказа первого элемента и коэффициента зависимости, учитывающего вероятность множественных человеческих ошибок.

Оценка параметров рассмотренных моделей — наиболее ответственная часть работы. Она включает следующие этапы [1, 3]:

сбор данных по отказам по общей причине, для чего необходима информация [20] о виде отказа, его причине, критичности для системы, времени обнаружения; желательно также знать тип отказавшего оборудования, место его расположения, завод-изготовитель, порядок обслуживания и другие данные для уменьшения субъективизма при оценках;

классификация событий из базы данных, для чего в работах [3, 9] предложено использовать диаграммы «причина — эффект»;

отбор событий из базы данных, имеющих отношение к анализируемой системе;

экспертная оценка характера их реализации на рассматриваемой системе; большое значение имеет распространение данных по системам с однократным резервированием на системы с другой кратностью резервирования; множественность события оценивается определением вектора воздействия, который является дискретным распределением вероятности числа элементов в группе, испытывающих воздействие при событиях [3,9];

количественная оценка параметра, например, с использованием байесовой процедуры.

Количественный анализ воздействий окружающей среды возможен следующим путем [1];

оценка интенсивности возникновения событий;

оценка подверженности элементов этим событиям (возможности проектных мер уменьшить или исключить их влияние) и возникающим нагрузкам;

оценка уязвимости (например, по кривым хрупкости) или несущей способности элементов, подверженных влиянию рассматриваемых событий;

сравнение несущей способности с предполагаемыми нагрузками для выявления отказавших элементов;

проведение вероятностных расчетов методами деревьев отказов и событий, исключая элементы, отказавшие при этих внешних событиях (или рассматривая соответствующие условные вероятности их отказов).

Защита против зависимых отказов

Основные защитные меры против зависимых отказов различных элементов, каналов или систем [1,23] следующие.

Физическое разделение резервируемых объектов. Эта мера эффективна при пожаре, разрывах труб, образовании летящих предметов, ударах молний, падении самолета и саботаже. Разделение должно касаться не только технологических, но и обеспечивающих и управляющих систем безопасности. Кроме того, оборудование нормальной эксплуатации и системы безопасности должны быть разделены с физической и функциональной точек зрения, что ограничивает распространение отказов. Дополнительное преимущество отсутствия взаимных связей между системами, выполняющими различные функции,— упрощение анализа безопасности и ускорение процесса лицензирования. В тех случаях, когда взаимосвязей между резервируемыми объектами избежать не удается, стремятся уменьшить возможности распространения отказа, например в логике управления это обеспечивают использованием оптоэлектрических устройств.

Разнопринципность (diversity) проекта, т. е. выполнение определенных функций безопасности различными системами, чье функционирование основано на различных проектных принципах. Часто это является эффективным средством защиты против отказов по общей причине, когда не помогает физическое разделение, т. е. против систематических ошибок при проектировании, изготовлении, монтаже и техническом обслуживании. Такая защитная мера обычно требует значительных затрат, поэтому, как правило, она используется только для жизненно важных функций безопасности.

Экспертиза проекта. К ней привлекается группа специалистов по различным областям: безопасности, механическому и электрическому оборудованию, монтажу и компоновке, эксплуатации. Системы безопасности анализируются комплексно и общение специалистов может выявить их слабые места. В случае необходимости проводятся также аналитические расчеты и эксперименты.

Периодические проверки работоспособности систем безопасности. Их проводят во время эксплуатации АЭС для выявления и устранения скрытых отказов, в том числе по общей причине. Их частота определяется технологическим регламентом. Обязательно также проведение проверок работоспособности оборудования после его ремонта. При выполнении оперативных переключений во время таких испытаний оборудования персонал может совершить оставшиеся незамеченными ошибки, которые станут общей причиной новых отказов. Такие последствия исключаются проведением проверок различных каналов систем безопасности в разное время, а также автоматическим возвращением элемента в исходное состояние после выполнения им своих функций.

Организационно-технические мероприятия. Основное значение придается адекватной программе обеспечения качества, обычно не требующей больших затрат. Организация четкого обмена устной и письменной информацией при проведении проверок и ремонтов оборудования — также важное мероприятие, минимизирующее потенциальные зависимые отказы, которые могут быть вызваны деятельностью персонала.

Стандартизация. Это эффективное средство повышения надежности оборудования, однако оно может увеличивать вероятность и влияние определенных типов отказов по общей причине, например, вызванных повторяющимися дефектами при изготовлении одинакового оборудования. Поэтому подобная мера защиты против зависимых отказов может привести к отрицательным результатам.

Специфические меры защиты против внешних экстремальных воздействий

Пожары, землетрясения, наводнения, падение самолета или образование летящих предметов могут вызвать множественные отказы резервируемого оборудования и привести к катастрофическим последствиям. Поэтому защите против экстремальных воздействий уделяется особое внимание [23].

В качестве противопожарной защиты используют, главным образом, пассивные средства: физическое разделение каналов систем безопасности, огнестойкие конструкции и материалы, сокращение количества горючих материалов. Так, на шведских серийных АЭС с BWR основные здания разделены на зоны, границы которых представляют собой огнестойкие конструкции. Каналы систем безопасности размещены в отдельных зонах, которые обслуживаются разными системами вентиляции. Этот принцип выдержан и для системы аварийной защиты реактора, оборудование которой расположено в четырех разных местах с раздельной вентиляцией, а на блочном щите управления оно размещено на разных стойках, имеющих противопожарную защиту.

При рассмотрении сейсмического риска определяется сила максимального проектного землетрясения, исходя из геологических особенностей площадки АЭС. Для сейсмической квалификации оборудования используются инженерные оценки, статические и динамические анализы, испытания.

Возможность наводнения зависит от площадки АЭС, поэтому для каждой станции проводят специфические анализы. Защита против такого воздействия связана с размещением оборудования, важного для безопасности, на таких отметках, куда вода от внешних источников не попадает даже в экстремальных условиях, как это сделано на шведской АЭС «Форсмарк-3». Для борьбы с внутренними затоплениями помещения АЭС оборудуются гидроизоляцией, используется диагностическое оборудование для своевременной локализации течи.

Основные методы защиты против падения самолета на АЭС заключаются в обеспечении прочности защитной оболочки и рассредоточении резервируемого оборудования. Специальное внимание уделяется анализу последствий возгорания авиационного топлива. Физического рассредоточения оборудования обычно достаточно, а там, где в реакторном отделении это невозможно, используется локальная защита.

Список литературы

1. **Amendola A.** Common cause failures analysis in reliability and risk assessment.— In: Reliability Engng. Proc. of Joint Research Centre ISPRA. Dordrecht: Kluwer Publisher, 1988, N 2.
2. **Hirschberg S.** Nordic benchmark and reference studies within the area of probabilistic safety analysis.— In: Proc. of IAEA Research Coordination Meet. on Reference Studies on Probabilistic Modelling of Accident Sequences, Moscow, 23—27.05.88.
3. **Fleming K., Mosleh A., Deremer R.** A systematic procedure for the incorporation of common cause events into risk and reliability models.— Nucl. Engng Des., 1986, v. 93, p. 245.
4. **Hirschberg S., Björe S., Jacobsson P.** Retrospective quantitative analysis of common cause failures and human interactions in Swedish PSA studies.— In: Proc, of Intern. Top. Meet. on Probability, Reliability and Safety Assessment, Pittsburg, USA, 2—7.4.89.
5. **Основные** принципы безопасности атомных электростанций. Сер. Безопасность, № 75, INSAG-3. Вена: МАГАТЭ, 1988.
6. **Vaurio J.** A procedure for parametric common cause failure assessment proposed for IAEA project RER/9/005.— In: Proc. of IAEA Workshop on Methodology and Data Base for VVER-PSA, Rer, CSSR, 12—17.6.88.
7. **Wright R.** Some data on common cause failures in redundancy industrial computer systems.— The Nucl. Engineer, 1986, v. 26, N 3, p. 72.
8. **Paula H.** A probabilistic dependent failure analysis of a D — C electric power system in a nuclear power plant.— Nucl. Safety, 1988, v. 29, N 2, p. 196.
9. **Procedures** for Treating Common Cause Failures in Safety and Reliability Studies. NUREG/CR-4780, EPRI, USA, Dec. 1988.
10. **Apostolakis G., Moieni P.** The foundation of models of dependence in probabilistic safety assessment.— Reliability Engng, 1987, v. 18, p. 177.
11. **Watson I.** Analysis of dependent events and multiple unavailabilities with particular reference to common cause failures.— Nucl. Engng Des., 1986, v. 93, p. 227.
12. **Johnston B.** A structured procedure for dependent failure analysis (DFA).— Reliability Engng, 1987, v. 19, p. 125.
13. **Parry G.** Comments on modelling uncertainty in parameter estimation.— Nucl. Safety, 1986, v. 27, p. 212.
14. **Dörre P.** An event-based multiple malfunction model.— Reliability Engng, 1987, v. 17, p. 73.
15. **Atwood C.** The binomial failure rate common cause model.— Technometrics, 1986, v. 28, N 2, p. 139.
16. **Hokstad P.** A shock model for common cause failures.— Reliability Engng and System Safety, 1988, v. 23, p. 127.
17. **Hughes R.** A framework for dependent failure analysis.— Ibid., 1989, v. 24, p. 139.
18. **Hughes R.** A new approach to common cause failure.— Reliability Engng, 1987, v. 17, N 3, p. 211.
19. **Hirschberg S., Jacobsson P., Pulkkinen U., Pörn K.** Nordic reference study on uncertainty and sensitivity analysis.— In [4].
20. **Hirschberg S.** Treatment of common cause failures. The Nordic perspective.— In: Proc. of Advanced Seminar on Common Cause Failures Analysis in Probabilistic Safety Assessment, JRC ISPRA, Italy, 16—19.11.87.
21. **Colas A.** Improving diesel generator reliability at French 900 MWe and 1300 MWe PWRs.— Nucl. Engng Intern., 1988, v. 33, N 406, p. 54.
22. **Škvarka P., Kandrač J., Lukač L.** Modelling of fire resistance reliability in nuclear power plants.— In: Proc. of IAEA Workshop on Advances in Reliability Analysis and Probabilistic Safety Assessment, Seregelyes, Hungary, 6—11.9.87.
23. **Hirschberg S., Tiven L.** Design-related defensive measures against dependent failures. ABB Atom's approach.— In [20].

Ключевые слова

Безопасность АЭС, зависимые отказы оборудования, методы качественного анализа, методы количественной оценки