2.9. Расчет надежности и эффективности системы с защитой

2.9.1. Описание задачи

Рассматривается конфигурация Объект (О) + Система Защиты (СЗ) (рис. 2.9.1.). Система защиты состоит в свою очередь из устройства контроля и исполнительного механизма.

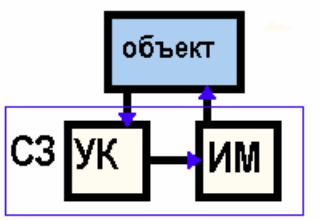

Рис. 2.9.1. Конфигурация Объект + Система Защиты

Рассмотрим более подробно работу и отказы в системе.

Подсистемы защиты предназначены для выработки управляющих воздействий на защищаемый объект (технологическое оборудование) с целью предотвращения развития нештатных отклонений в работе объекта и, в частности, перерастания отказов в аварию (здесь будем рассматривать только отклонения в работе объекта, связанные с отказами).

Управляющие воздействия могут быть различными (напр., изменение режима работы, снижение производительности). В некоторых случаях они реализуют отключение аварийно отказавших элементов и других элементов, связанных с первыми по технологической цепи. Тем самым предотвращается развитие событий, приводящих к аварии. Как правило, это бывает эквивалентно останову объекта, технологического процесса. Здесь будем рассматривать именно такой случай, но предлагаемый подход годится и для управляющих воздействий, приводящих к снижению производительности, изменению режима.

Функция противоаварийной защиты выполняется эпизодически, в момент возникновения аварийной ситуации, поэтому подсистема защиты (СЗ) работает в ждущем временном режиме. Характер доходов в работоспособных состояниях и потерь в неработоспособных состояниях объекта (О) предполагается следующим. Во-первых, в системе (в данном примере это О + СЗ) возможны четыре группы технических состояний (техническое состояние характеризуется наборами отказавших и работоспособных элементов модели (СЗ, О), видами и последовательностью возникновения отказов). Первая группа содержит такие технические состояния, в которых объект нормально функционирует и приносит удельный доход в единицу времени пребывания в этих состояниях (напр., этим состояниям соответствует номинальная производительность О). Отметим, что в эту группу входят состояния со скрытым отказом (типа несрабатывания на требование) подсистемы защиты. Вторая группа состояний характеризуется безаварийным остановом объекта. Потери здесь связаны только с простоем объекта; доход в этих состояниях либо равен нулю, либо отрицательный, если простой приводит к дополнительным потерям в единицу времени. Третья и четвертая группы состояний – аварийные отказы объекта двух видов. Переход в эту группу состояний из состояний первой группы приносит единовременный ущерб (отрицательный доход) связанный с возникновением аварии (гибель людей, поломки оборудования, выбросы в атмосферу и т.п.). Таким образом, нормальное функционирование объекта сопровождается линейным ростом интегрального дохода пропорционально времени пребывания в первой группе состояний. Простои объекта в состояниях второй, третьей и четвертой групп ведут к сохранению достигнутого уровня интегрального дохода

(при нулевых значениях удельных доходов в каждом из состояний этих групп) либо к его убыванию (при отрицательных значениях соответствующих удельных доходов) пропорционально времени пребывания в этих состояниях. При переходах между состояниями имеет место скачкообразное изменение (чаще уменьшение) интегрального дохода в тех случаях, когда с соответствующими переходами связаны единовременные доходы за каждый переход, Обычно эти доходы отрицательны, обусловлены затратами на восстановление последствий отказов, аварий, приобретение оборудования, ЗИП′а, штрафы, страховку и т.п.

Предположим, что все аварийные ситуации (АС) возникают только при отказах технологического оборудования. Пусть СЗ при возникновении распознаваемой ей АС мгновенно останавливает технологический процесс, производя необходимое управление оборудованием (например, отключение). Причем работоспособная СЗ с ″покрытием″ β ($0 \le \beta \le 1$) распознает аварийные ситуации. Отказы в СЗ, которые возникают на интервале нормального функционирования О, могут приводить к различным последствиям. Выделим отказы двух видов: скрытые отказы и ложные срабатывания. Скрытые отказы не приводят к срабатыванию защиты и не изменяют режим работы объекта. Они проявляются в виде несрабатывания защиты при возникновении АС, что влечет за собой аварию.

Параметры модели:

Wij – потери от переходов в состояния аварии;

β - “покрытие”- доля распознаваемых аварийных ситуаций работоспособной СЗ;

α - доля скрытых отказов устройств СЗ типа «несрабатывание»;

1-α - доля явных отказов устройств СЗ типа «ложное срабатывание»;

η1, η2 – доля аварийных отказов I и II рода О;

λ, μ - интенсивности отказов и восстановления СЗ, О.

Рассматриваемая система (О + СЗ) имеет 4 подмножества состояний:

- нормальное функционирование;
- останов (безаварийный);
- авария I;
- авария II.

Необходимо сделать расчет средних рисков на интервале (t =0 ÷ 1000ч) для трех значений параметра β. Рассматриваются случаи наличия и отсутствия восстановления из состояний аварий. Среднее время восстановления из аварии I - 5суток. Среднее время восстановления из аварии II - 10суток. Ущербы от перехода в состояние аварии II равны 8 баллов, в состояние аварии I - 4 балла.

2.9.2. Результаты решения на ПК «RELEX»

Граф переходов марковской модели представлен на рис. 2.9.2.

Интенсивности переходов:

$\lambda_{12} = [1 - (1 - \beta) \cdot (\eta_1 + \eta_2)] \cdot \lambda_o + (1 - \alpha_к) \cdot \lambda_к + (1 - \alpha_{им}) \cdot \lambda_{им}$;
$\lambda_{13} = \alpha_к \cdot \lambda_к$;
$\lambda_{14} = \alpha_{им} \cdot \lambda_{им}$;
$\lambda_{15} = (1 - \beta) \cdot \eta_1 \cdot \lambda_o$;
$\lambda_{17} = (1 - \beta) \cdot \eta_2 \cdot \lambda_o$;
$\lambda_{21} = \lambda_{61} = \mu$;
$\lambda_{32} = (1 - \eta_1 - \eta_2) \cdot \lambda_o + (1 - \alpha_{им}) \cdot \lambda_{им}$;
$\lambda_{37} = \lambda_{47} = \eta_2 \cdot \lambda_o$;
$\lambda_{35} = \lambda_{45} = \eta_1 \cdot \lambda_o$;
$\lambda_{46} = (1 - \eta_1 - \eta_2) \cdot \lambda_o$.

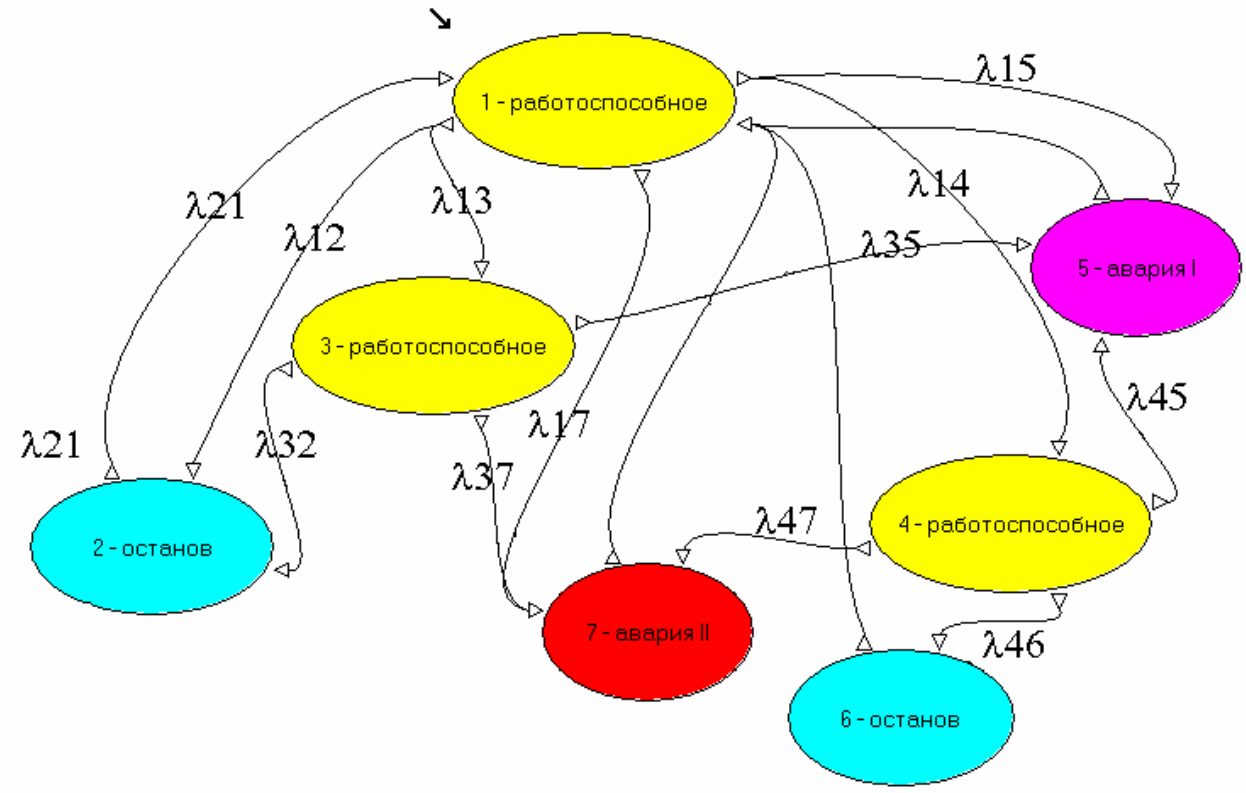

Рис. 2.9.2. Граф переходов состояний Марковской модели в Relex Markov

Значение параметров модели:

$\lambda o = 0.005$; $\lambda к = 0.001$; $\lambda им = 0.002$; $\alpha к = 0.3$; $\alpha им = 0.5$; $\eta 1 = 0.4$; $\eta 2 = 0.3$; $\mu = 0.05$.

Балльная оценка ущербов произведена по результатам проведения экспертами качественного анализа видов и последствий отказов (модуль Relex FMEA/FMECA) (см. таблицу 2.9.1).

Таблица 2.9.1.

Характеристика последствий отказа	ВЗ, баллы
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, взрыв, образование токсического облака, цепное развитие аварии на промплощадке предприятия и за его пределами. Среди персонала и населения могут быть жертвы; есть необходимость эвакуации населения; окружающая среда получит значительный ущерб; объект – полное разрушение; остановка производства может быть 1 месяц и более.	**9 - 10**
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, взрыв, повреждение близлежащего оборудования, развитие аварии не выходит за пределы предприятия. Среди персонала могут быть травмированные; возможна эвакуация населения и нанесение восполнимого ущерба окружающей среде, остановка производства более 10 суток.	**7 - 8**
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, развитие аварии не выходит за пределы технологической установки. Персонал может получить незначительные травмы; население – опасности нет; окружающая среда – ущерба нет; остановка производства более 5 суток.	**5 - 6**
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, развитие аварии не выходит за пределы технологического блока. Персонал может получить незначительные травмы; население – опасности нет; окружающая среда – ущерба нет; остановка производства более суток	**3 – 4**
Отказ вызывает незначительную разгерметизацию аппарата, загорание непосредственно в пределах аппарата. Персоналу, населению, окружающей среде угрозы нет; остановка производства менее суток.	**1 - 2**

Результаты расчетов средних рисков на интервале (t =0 ÷ 1000ч) приведены в таблице 2.9.2.

Таблица 2.9.2.

β		с СЗ	без СЗ
0.8	с восстановлением	**-5.3**	**-12**
	без восстановления	**-3.9**	**-5.5**
0.99	с восстановлением	**-2.9**	**-12**
	без восстановления	**-2.6**	**-5.5**
1	с восстановлением	**-2.8**	**-12**
	без восстановления	**-2.5**	**-5.5**

2.9.3. Результаты решения на ПК «АСМ»

В технологии и ПК АСМ методы и средства автоматизированного марковского моделирования в настоящее время не реализованы.

2.9.4. Результаты решения на ПК «RISK SPECTRUM»

Программный комплекс «Risk Spectrum» предназначен для выполнения ВАБ АЭС, т.е. для анализа показателей надежности и безопасности технических систем, включающих в свой состав тысячи единиц оборудования, могущих находится в сотнях эксплуатационных состояний (режимов использования) и т.п. Естественно, что это накладывает определенные требования на используемое математическое и программное обеспечение.

Специалистами института «Атомэнергопроект» (г. Москва) производились исследования возможности использования марковских методов для решения указанного класса задач, см. например, Клемин А.И., Емельянов В.С., Морозов В.Б. Расчет надежности ядерных энергетических установок. Марковская модель. С.: Энергоиздат, 1982., Клемин А.И. Надежность ядерных энергетических установок. основы расчета. М.: Энергоатомиздат, 1987. В ходе этих исследований установлено, что для решения реальных задач ВАБ марковские методы практически не применимы вследствие ограничений на размерность соответствующих математических моделей.

Эти выводы подтверждаются исследованиями И.А. Рябинина, см. например, Рябинин И.А., Китушин Ю.Н. Надежность судовых электроэнергетических систем и судового электрооборудования. Л.: Судостроение, 1974. В данном труде указывается (см. стр. 174), что общее число состояний СЭС, рассмотренной нами в разделе 2.1, составляет 32 768. Полный набор всех путей, выраженных в СДНФ, насчитывает 2410 членов, из которых 92 являются кратчайшими. Такие цифры вызывают естественное сомнение в возможности построения марковского графа переходов для такой системы, а также в возможности получения аналитического решения, имеющего приемлемую точность. В любом случае, требуемый результат (расчет показателей надежности СЭС) может быть достигнут с меньшими усилиями при использовании альтернативных методов.

Учитывая назначение кода «Risk Spectrum», а также то, что реальные системы АЭС значительно сложнее СЭС, рассмотренной в п. 2.1, и основываясь на неофициальной информации специалистов СПбАЭП о планах развития данного кода, можно утверждать, что классы задач, рассмотренные выше в данном разделе и решенные модулем марковского анализа (Relex Markov) в технологии «Risk Spectrum» реализованы не будут ввиду отсутствия практической надобности.

Сводная таблица результатов раздела 2.9. " Расчет надежности и эффективности системы с защитой "					
Relex FMEA/FMECA				ПК АСМ	Risk Spectrum
1				2	3
Балльная оценка ущербов произведена по результатам проведения экспертами качественного анализа видов и последствий отказов				не выполняется	не выполняется
Характеристика последствий отказа			В3, баллы		
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, взрыв, образование токсического облака, цепное развитие аварии на промплощадке предприятия и за его пределами. Среди персонала и населения могут быть жертвы; есть необходимость эвакуации населения; окружающая среда получит значительный ущерб; объект – полное разрушение; остановка производства может быть 1 месяц и более.			**9 - 10**		
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, взрыв, повреждение близлежащего оборудования, развитие аварии не выходит за пределы предприятия. Среди персонала могут быть травмированные; возможна эвакуация населения и нанесение восполнимого ущерба окружающей среде, остановка производства более 10 суток.			**7 - 8**		
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, развитие аварии не выходит за пределы технологической установки. Персонал может получить незначительные травмы; население – опасности нет; окружающая среда – ущерба нет; остановка производства более 5 суток.			**5 - 6**		
Отказ вызывает разгерметизацию аппарата, выброс опасной среды из аппаратуры, пожар, развитие аварии не выходит за пределы технологического блока. Персонал может получить незначительные травмы; население – опасности нет; окружающая среда – ущерба нет; остановка производства более суток			**3 – 4**		
Отказ вызывает незначительную разгерметизацию аппарата, загорание непосредственно в пределах аппарата. Персоналу, населению, окружающей среде угрозы нет; остановка производства менее суток.			**1 - 2**		
Результаты расчетов средних рисков на интервале (t =0 ÷ 1000ч)				не выполняется	не выполняется
β		с СЗ	без СЗ		
0.8	с восстановлением	**-5.3**	**-12**		
	без восстановления	**-3.9**	**-5.5**		
0.99	с восстановлением	**-2.9**	**-12**		
	без восстановления	**-2.6**	**-5.5**		
1	с восстановлением	**-2.8**	**-12**		
	без восстановления	**-2.5**	**-5.5**		

ВЫВОДЫ ПО РАЗДЕЛУ 2.9

Выводы специалистов ИПУ РАН

В разделе рассматривалась довольно сложная модель, учитывающая последовательность возникновения отказов, некоторые виды несовместности и различные уровни эффективности функционирования (в частности, ущерба). Задача решена только на ПК Relex.

Выводы специалистов ОАО "СПИК СЗМА"

1. В технологии и ПК АСМ методы и средства автоматизированного марковского моделирования в настоящее время не реализованы.

2. Вместе с тем, хотелось бы отметить, что специалистами Компании в настоящее время получены первые успешные решения задач автоматического построения графов переходов состояний марковских моделей большой размерности, расчета параметров переходов и получения с помощью ЭВМ соответствующих матриц переходных вероятностей, лямбда-матриц, систем алгебраических и дифференциальных уравнений. Исходными данными в решении задач данного класса выступают те же схемы функциональной целостности, логические критерии функционирования и параметры элементов. Размеры автоматически формируемых марковских моделей достигают нескольких сотен состояний и нескольких десятков и сотен тысяч переходов. В настоящее время марковские модели могут автоматически строиться без учета и с учетом групп несовместных событий.

3. Разработаны и автоматизированы методы расчета на основе автоматически формируемых цепей Маркова условных законов живучести и условных законов поражения систем, подвергающихся заданным последовательностям различных поражающих воздействий.

4. Методы и средства автоматического построения и расчета высокоразмерных марковских моделей с непрерывным временем находятся в стадии разработки и не внедрены в программные комплексы автоматизированного структурно-логического моделирования.

5. Мы считаем данное направление работ актуальным и перспективным.

Выводы специалистов СПбАЭП

1. Пример 2.9, демонстрирующий применение марковских процессов для учета последовательности возникновения отказов, решен только с помощью ПК «Relex».

2. В технологии АСМ выполнены теоретические проработки и созданы первые программные реализации некоторых разделов марковского моделирования. Решение задачи, рассмотренной в данном примере в ПК АСМ в настоящее время не реализованы.

3. В связи с отсутствием практической надобности в решении задач, подобных рассмотренной в данном разделе, при производстве ВАБ АЭС, реализация их в технологии «Risk Spectrum» не планируется.