УДК 004.052

Ирадж Эльяси Комари

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

ПРИМЕНЕНИЯ FME(C)A-АНАЛИЗА ДЛЯ ОЦЕНКИ И ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ СЛОЖНЫХ ИЕРАРХИЧЕСКИХ КОМПЬЮТЕРНЫХ СИСТЕМ

Предложены варианты совершенствования оценки надежности сложных иерархических компьютерных систем с использованием иерархии FME(C)A-таблиц. Проанализированы способы формирования интегральных показателей критичности отказов, а также предложена методика выбора средств для снижения критичности отказов.

компьютерные системы, надежность, анализ видов и причин отказов, FME(C)A

Введение

Проблема оценки надежности сложных компьютерных систем. В настоящее время все большие сферы человеческой деятельности становятся зависимыми от качества и надежности компьютерных систем, применяемых для автоматизации различных процессов. Среди множества компьютерных систем особое внимание заслуживают системы, важные для безопасности, или критические компьютерные системы (ККС).

К таким системам можно отнести любую систему, сбой или отказ в работе которой может привести к нанесению серьезного ущерба окружающей среде, большим финансовым потерям и даже гибели людей. Примерами ККС являются навигационные системы самолётов и морских судов, информационно-управляющие системы атомных электростанций и вредных химических производств, компьютерные системы аэрокосмических комплексов и т.п.

Применительно к ККС обычно говорят не о безопасности или надёжности системы, а о риске возникновения аварии (accident risk). Задача разработчика ККС заключается в том, чтобы оценить величину риска аварии и по возможности снизить её до некоторого приемлемого уровня; при этом, при выборе вариантов построения системы и применения средств защиты от отказов, разработчик должен учитывать общую стоимость системы.

Анализ литературы. Постановка задачи. Существует несколько способов выявления возможных отказов системы и оценки риска аварий. На практике чаще других используются FME(C)A (Failure Modes and Effects (Critical) Analysis), FTA (Fault Tree Analysis) [1] и FTA (Fault Tree Analysis) [2]. Это известные методы, которые были успешно применены в различных областях для рассмотрения причин и последствий системных отказов [4]. В работе [5] этот метод обобщен на случай web-сервисов, учитывает информационные воздействия на систему и поэтому получил название F(I)MEA-процедур (Failure and Intrusion Modes and Effects Analysis). Обычно FME(C)A-методика позволяют проанализировать виды и последствия первых (одиночных) отказов. В то же время для ККС бывает важно оценить их надежность с учетом возможных кратных отказов и последовательностей одиночных и/или кратных отказов. Для этого могут использоваться иерархии FME(C)A-таблиц [6]. Но даже анализ одиночных отказов и их влияние на работу всей системы и отдельных её компонент может стать нетривиальной задачей, когда речь идет о сложной иерархической компьютерной системе.

Именно с факторами усложнения разрабатываемых систем и появлением критических компьютерных систем и интенсивным использованием программного обеспечения связано проявление недостатков указанных методов.

Так, на первом этапе FME(C)A-анализа должны быть сформированы сводные таблицы, включающие: перечень и классификацию возможных отказов объекта по видам, причинам и условиям возникновения, их последствиям и уровню критичности. Для сложных компьютерных систем это приводит к большой размерности FMECA-таблиц, что в свою очередь влияет на сложность анализа и учета взаимосвязей между подсистемами и возможностей распространения влияния отказов. Что касается методики построения и анализа деревьев отказов, то FTA не учитывает различную степень критичности отказов в дереве, а также то, что последствием отказа может стать не только полная потеря работоспособности, но и частичная.

Кроме того, в методике не отражен тот факт, что отказ более верхнего уровня дерева FTA может являться следствием определенных отказов нижнего уровня не всегда, а с некоторой вероятностью при возникновении определенных внешних или внутренних событий.

Цель статьи – анализ путей модернизации методики анализа видов и последствий отказов

 © Ирадж Эльяси Комари

FME(C)A для оценки сложных компьютерных систем, оптимального выбора средств защиты от отказов, а также взаимодействие с методикой FTA.

Построение иерархии FME(C)A-таблиц

Для устранения недостатка размерности при использовании единой FMEA-таблицы для анализа сложных иерархических компьютерных систем предлагается перейти к построению иерархии FME(C)A-таблиц. Такая иерархия может отражать структуру системы и строиться по уровням «подсистемы» – «элементы подсистем» – «компоненты элементов», как это показано на рис. 1:

– первая таблица рассматривает отказы отдельных подсистем системы;

– таблица первого уровня вложенности рассматривает отказы отдельных элементов каждой конкретной подсистемы;

– таблица второго уровня вложенности рассматривает отказы отдельных компонентов каждого конкретного элемента системы и т.д.

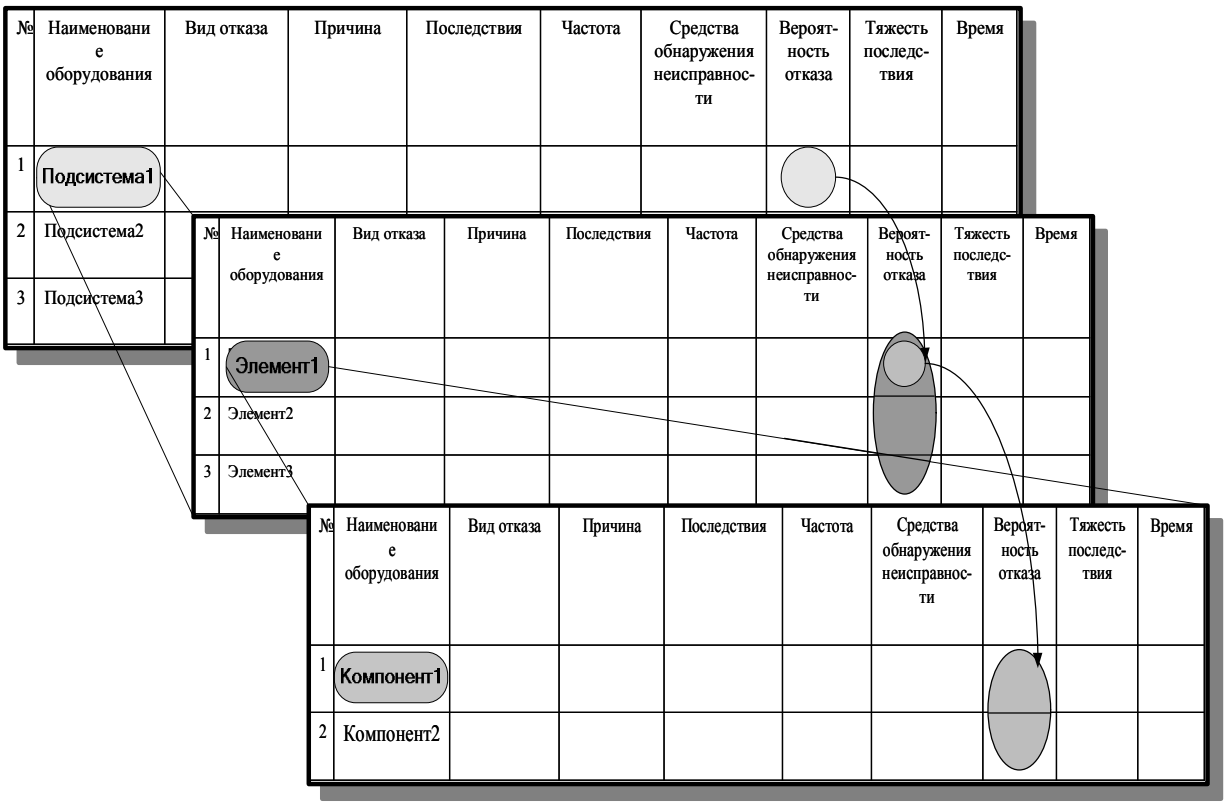

Рис. 1. Иерархия FME(C)A-таблиц

Кроме того, на верхнем уровне целесообразно отделить программное и аппаратное обеспечение, в силу специфичности причин и последствий их отказов.

Вторым возможным подходом является декомпозиция FME(C)A-таблиц по функциям, реализуемым системой.

Интегральная оценка критичности отказов

Традиционно для оценки критичности отказов использовались два фактора [1]: тяжесть последствия отказа и вероятность его возникновения. Чем выше оба значения, тем критичнее отказ. В [4] для оценки критичности современных компьютерных систем было предложено использовать третье измерение, отражающее влияние отказа на готовность – время неработоспособности системы после отказа. Однако теперь, с появлением иерархии FME(C)A-таблиц, необходимо решить вопрос, как в иерархии таблиц будет оцениваться интегральная тяжесть последствий, вероятность возникновения, а также продолжительность неработоспособности для каждого конкретного отказа?

Например, необходимо оценить тяжесть последствий и вероятность возникновения отказа подсистемы 1 (рис. 1) с учетом характеристик отказов элементов этой подсистемы.

Здесь возможны несколько вариантов:

1. Вероятность отказа верхнего уровня иерархии считается как произведение всех вероятностей отказов из вложенной таблицы.

Недостаток этого способа заключается в том, что он не позволяет учесть внутренней связи элементов.

2. Вероятность отказа на верхнем уровне рассчитывается с помощью построения дерева отказов FTA для вложенной таблицы.

Этот способ является более точным и позволяет учесть взаимосвязь отказавших элементов (посредством применения элементов OR, AND и т.д.).

3. Тяжесть последствий может оцениваться как средняя тяжесть отказов из вложенной таблицы или браться две оценки – пессимистическая и оптимистическая или же, как тяжесть наиболее вероятного отказа или же взвешенная тяжесть отказов с учетом их вероятности возникновения.

Тяжесть последствий отказа объекта и причину его появления устанавливают обычно для объекта на высшем уровне иерархии в виде более общего заключения об отказе подсистем следующих уровней, а затем начинают анализ подсистем.

Процесс анализа идет далее с большой конкретизацией данных об элементах более низкого уровня.

Как видно на рис. 1, вложенная таблица подсистемы 1 может иметь несколько элементов, которые, в свою очередь, могут иметь разную тяжесть последствий и разную вероятность отказа.

Для того чтобы определить интегральную тяжесть последствия, можно использовать взвешенную тяжесть отказов с учетом их вероятности возникновения:

$$Тпосл_{\Sigma} = \sum_{i=1}^{N} Тпосл_i \times Q_i \,. \qquad (1)$$

Недостатком такой оценки является отсутствие понятия «веса оценки», в результате чего отказы с малыми вероятностями возникновения и тяжелыми последствиями и отказы с высокими вероятностями возникновения и незначительными последствиями имеют одинаковую оценку критичности, т.е. общая оценка не дает реальной картины происходящего.

Интегральная оценка времени неработоспособности также может быть оценено по формуле (1) с учетом вероятности возникновения каждого отказа.

Выбор средств снижения критичности отказов

Основной целью применения FME(C)A-методики является систематизация возможных отказов системы и выявление среди них наиболее критических с помощью построения матриц критичности [3, 4].

Следующим, менее формализованным шагом является выбор эффективных средств снижения их критичности до некоторого, приемлемого уровня. Это может быть сделано комплексным применением средств предупреждения, предотвращения и парирования отказов, а также средств автоматического или автоматизированного восстановления после отказов и снижения тяжести их последствия:

1. Средства уменьшения вероятности возникновения:

а) необходимости повышения качества и надежности компонентов системы. Здесь речь идёт о внедрении в систему резервных, а также более качественных (и более дорогих) компонентов;

б) применения в облегченном режиме;

в) введения защиты от перегрузок, дополнительных проверок и испытаний в процессе изготовления и эксплуатации.

2. Средства уменьшения тяжести последствий:

а) изменение структуры системы и применения дополнительных схемотехнических решений (например, систем аварийной защиты, как на АЭС, когда при обнаружении любого отказа эта система глушит реактор, или сторожевых таймеров, которые в случае, если система долго не отвечает, перезагружают ее);

б) использование внутренних предохранительных устройств, позволяющих снизить риск возникновения аварии в том случае, если отказ каких-либо компонентов системы уже произошёл;

в) использование внешних предохранительных устройств. Они применяются в случае, если произошло некоторое опасное событие (hazard), которое может непосредственно повлечь возникновение самой аварии;

г) применение мер, относящихся к системам противоаварийной защиты и контроля (например, применение анализаторов, сигнализации и др.).

3. Средства уменьшение времени неработоспособности:

а) применения автоматизированных или автоматических средств диагностирования и восстановления после отказов (например, в компьютерных сетях вместо статических таблиц маршрутизации использовать протоколы динамической маршрутизации; оповещение о разрыве сетевого соединения).

Методика анализа отказов и выбора средств снижения их критичности

Методика применения FME(C)A-анализа для оценки и обеспечения надежности сложных иерархических компьютерных систем показана на рис. 2.

На первом этапе выполняется анализ видов и последствий отказов и формирование иерархии FMEA-таблиц в соответствии со структурой анализируемой системы.

На втором этапе выполняется анализ параметров отказов, влияющих на критичность (вероятность возникновения, тяжесть продолжительность неработоспособности).

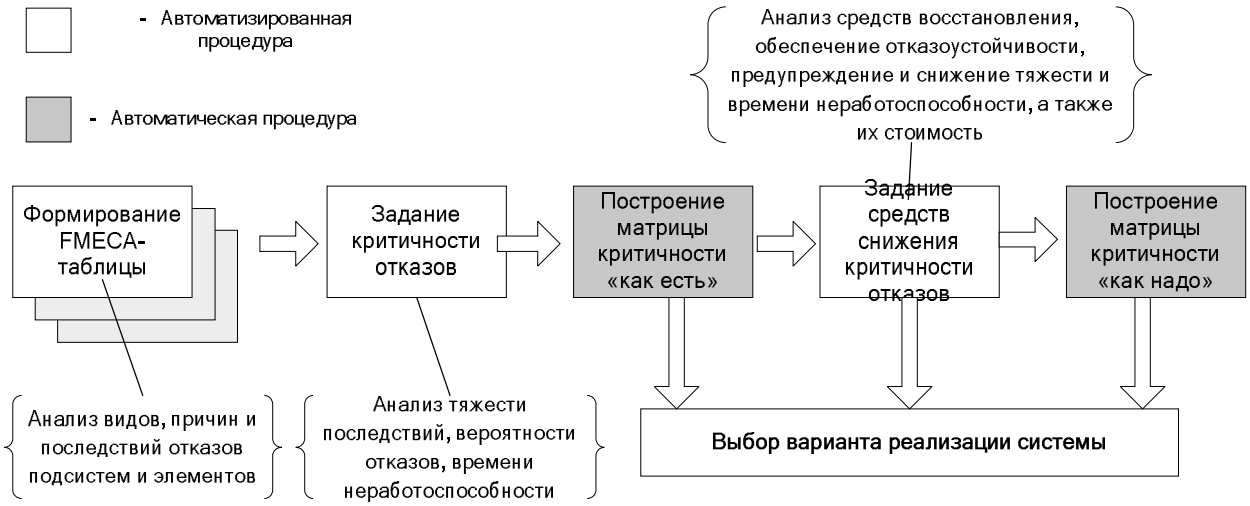

Рис. 2. Методика анализа отказов и выбора варианта построения системы

Затем для каждого отказа определяется набор средств по снижению критичности, причем для каждого средства необходимо проанализировать степень снижения критичности, возможность совместного использования нескольких средств, а также задать стоимость.

Следующая процедура собственно расчета критичности каждого отказа и построения исходной матрицы критичности может быть полностью автоматической.

Наконец, последним этапом является выбор из всего множества конкретных средств снижения критичности каждого конкретного отказа, построение результирующей матрицы критичности и анализ стоимости реализации системы. Эта процедура может быть итерационной и выполняться аналитиком или же использовать программно-реализуемые средства для автоматического поиска решений, основанные на методах дискретной оптимизации.

Заключение

Традиционные методы анализа видов и последствий отказов FME(C)A и FTA должны быть усовершенствованы с учетом современных особенностей разработки компьютерных систем (сложность, иерархичность, интенсивное использование ПО), их назначения (системы, важные для безопасности, системы высокой готовности) и среды работы.

Перспективным видится совместное применение методов FME(C)A и FTA, что позволит выполнить взаимное отображение между получаемыми с их помощью результатами анализа надежности, а также дополнить друг друга недостающей информацией.

На базе предложенной методики FME(C)A-анализа для оценки и обеспечения надежности сложных иерархических компьютерных систем разрабатывается инструментальное средство, позволяющее автоматизировать основные процедуры.

Список литературы

1. ГОСТ 27.310-95 (МЭК 812-1985). "Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения". – М.: Изд-во стандартов, 1997. – 12 с.

2. IEC 1025-1990. Fault tree analysis (FTA) / Стандарт МЭК "Анализ дерева отказов", 1990. – 36 с.

3. Kharchenko V., Gorbenko A. FME(C)A Technique of Assessment and Ensuring of a Corporate Computer Network Fault-Tolerance and Safety // 6th Probabilistic Safety Assessment and Management Conf., Puerto Rico, 2002. – P. 45-52.

4. Ирадж Эльяси Комари, Горбенко А.В. Анализ задач разработки и реинжиниринга компьютерных сетей для критических приложений // Радіоелектронні і комп'ютерні системи. – 2006. – № 7 (19). – С. 32-35.

5. Gorbenko A., Kharchenko V., Tarasyuk O., Furmanov A. F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring. LNCS4157. Development of Complex Fault-Tolerant Systems. Butler M., Jones C., Romanovsky A., Trubitsyna E. (eds.). – Springer. – 2006. – P. 153-168.

6. Ирадж Эльяси Комари. Метод анализа надежности компьютерных сетей сервисов с использованием FME(C)A-иерархий // МНТК "Інтегровані комп'ютерні технології в машинобудуванні". – Х.: Нац. аерокосм. ун-т «ХАІ», 2006. – С. 275-276.

Поступила в редколлегию 24.12.2007

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.