УДК 685.1

Харченко В.С., д-р техн. наук
Ирадж Эльяси Комари

КОМПЛЕКСНЫЙ АНАЛИЗ ГАРАНТОСПОСОБНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ И ИНФРАСТРУКТУР: FME(C)A-МОДЕЛИ И ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

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

Проанализирован FME(C)A-подход к оценке надежности и безопасности информационно-управляющих систем и инфраструктур. Предложены модели FME(C)A-таблиц для оценки свойств гарантоспособности (надежности, живучести и безопасности) и элементы информационной технологии анализа информационно-управляющих систем

Введение

Одной из важных научных и практических задач является оценка и обеспечение надёжности и безопасности сложных информационно-управляющих систем (ИУС) для критических приложений (нефтегазовых комплексов, авиационных и ракетно-космических систем, атомных электростанций и др.). Существуют различные математические методы оценки надёжности ИУС, базирующиеся на аппарате марковских и полумарковских процессов, имитационного моделирования [1] и др.

В последнее десятилетие интенсивно развиваются методы формализованной оценки, базирующиеся на анализе критичности отказов – *FME(C)A*, построении деревьев отказов и событий – *FTA*, анализе аварийных ситуаций - *HAZOP* [2,3] и др.

Ключевым среди них является, на наш взгляд, метод, основанный на построении *FME(C)A* (*Failure Modes, Effects* (*and Criticality*) *Analysis*)-таблиц, позволяющих представить в виде систематизированного списка информацию о причинах и видах отказов для различных компонент ИУС и их последствиях, оцениваемых в пространстве «вероятность-тяжесть» с помощью специальной матрицы критичности. В [4] показано, каким образом осуществляется переход от *FME(C)A*-таблиц к построению марковских моделей надежности (готовности) для сетевых структур.

Проведенный анализ позволяет сделать вывод, что возможности *FME(C)A*-подхода для оценки свойств ИУС далеко не исчерпаны. Это подтверждается публикациями, в которых показана целесообразность его применения для оценки информационной безопасности с использованием так называемой *F(I)MEA* (*Failure*(*Intrusion*) *Modes and Effects Analysis*)-методики, оценки последствий отказов с точки зрения времени восстановления [5].

Цель статьи – разработка предложений по расширения возможностей использования *FME(C)A*-подхода для комплексного анализа гарантоспособности сложных ИУС на различных этапах их жизненного цикла и элементов информационной технологии, поддерживающей такой анализ.

FME(C)A-модель и пути её расширения

Классическая *FME(C)A*-таблица является *списком FT*, который может быть представлен множеством из F векторов (числом строк таблицы – элементов системы):

$$FT=\langle e_f, c_f, r_f, p_f, u_f\rangle_{f=1}^{F}, \qquad (1)$$

где e_f – отказавший элемент (причина отказа);
c_f – вид отказа;
r_f – последствия (проявление) отказа;
p_f, u_f – вероятность и тяжесть отказа соответственно, которые могут задаваться на нечёткой шкале (например, «высокий» – «средний» – «низкий»).

Модернизация модели *FT* может быть выполнена в части расширения (уточнения):

- оцениваемых объектов (элемент-компонент, система, инфраструктура);
- учитываемых причин (дефектов и видов воздействий);
- оцениваемых последствий (вероятность, тяжесть, время восстановления);
- оцениваемых свойств (безопасность, готовность, безопасность – информационная и функциональная, живучесть);
- используемых средств (устойчивости к различным отказам, воздействиям);
- оцениваемым процессам (анализ, разработка, реинжиниринг).

Далее проведём расширение модели (1) с учётом этих элементов.

Объект FME(C)A-анализа

Объектами анализа, основанного на *FME(C)A*- методике, являются, как правило, компоненты ИУС – аппаратные и программные средства. Для программных средств разработана модификация этой методики – *SFME(C)A* [6]. В [4] предложено распространить *FME(C)A*-анализ на иерархические структуры, которым ставится в соответствие иерархия *FME(C)A*-таблиц.

Таким образом, в качестве объекта *FME(C)A*-анализа следует рассматривать иерархическую ИУС как «систему систем» или *инфраструктуру – IS* (рис. 1), при разработке которой может базироваться на парадигме «гарантоспособная система из негарантоспособных компонент» [7].

В этом случае от одиночной таблицы *FT*, описываемой моделью (1), следует перейти к их иерархии FT_{IS}, описываемой набором вложенных множеств компонент системы:

$$FT_{IS} = \{FT_{Sk} = \{FT_{HWk} = \{FT_{HWki}\}_{i=1}^{nk}, FT_{SWk} = \{FT_{SWkj}\}_{j=1}^{mk}\}\}_{k=1}^{k}, \quad (2)$$

где FT_{Sk} – модель (таблица) системы S_k, $k=\overline{1,K}$ (K – число систем (подсистем) инфраструктуры *IS*);

FT_{HWk}, FT_{SWk} – модели (таблицы) для аппаратных и программных средств подсистемы S_k;

FT_{HWki}, FT_{SWkj} – модели (таблицы) i-той аппаратной и *j*-той программной компонент ($i=\overline{1,n_k}$, $j=\overline{1,m_k}$).

Причины и последствия отказов

Отказ ИУС может произойти вследствие *физических дефектов* (*physical faults*) аппаратных средств, *проектных дефектов* (*design faults*), как правило, программных средств, и *внешних воздействий* (*interaction faults*) физического или информационного характера [8]. Физические (проектные) дефекты описываются в рамках модели (1) для аппаратных (программных) средств элементами e_f, c_f, r_f.

При таком анализе ключевым является вопрос определения *последствий* отказа, т.е. указания либо функции, которую не может выполнить система, либо показателя качества, который снижается вследствие такого отказа.

Отказы, обусловленные внешними воздействиями, могут описываться с помощью дополнительного элемента модели – v_f. К числу таких воздействий относятся механические, электромагнитные и другие физические воздействия $v(ф)_f$, а также непредумышленные (ошибки персонала) или целенаправленные (спам, хакерские атаки) информационные воздействия $v(x)_f$.

Таким образом, модель (1) может быть дополнена следующим образом:

$$FT=\langle v_f, e_f, c_f, r_f, p_f, u_f \rangle_{f=1}^{F}. \quad (3)$$

Для обслуживаемых ИУС критического применения очень важным показателем, который оценивается при анализе отказов, является время восстановления,

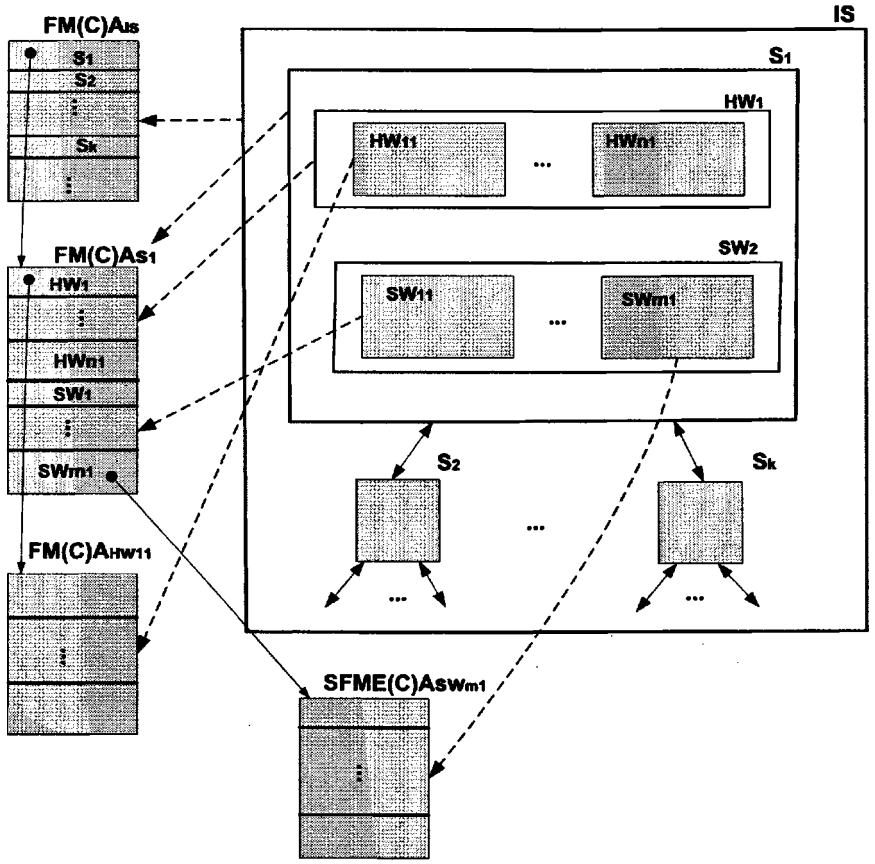

Рис. 1. Объект *FME(C)A* – анализа

t_f, которым следует дополнить выражение (3):

$$FT=<v_f,e_f,c_f,r_f,p_f,u_f,t_f>_{f=1}^{F}. \qquad (4)$$

Учёт показателя t_f обуславливает переход от матрицы («квадрата») критичности (рис. 2), описывающей последствия отказа в двухмерном пространстве «вероятность - тяжесть», к *«кубу» критичности* – трёхмерной матрице в пространстве «вероятность – тяжесть – время восстановления (устранения последствий отказа)» (рис. 2). На рис. 2 принята трехуровневая шкала для значений показателей: низкое (Н), среднее (Ср), высокое (В). На рис. 2,а матрица содержит следующие степени критичности в зависимости от комбинаций значений вероятности и тяжести последствий: 1 – катастрофическая, 2 – критическая, 3 – средняя критичность, 4 – незначительная, 5 – некритическая. На рис. 2,б количество градаций критичности может быть больше с учетом комбинаций значений трех показателей.

Оцениваемые свойства и используемые средства

FME(C)A – подход используется для оценки:

– *безотказности* ИУС, когда модель (1) может включать только часть элементов, а именно e_f, c_f, r_f, p_f,

– *готовности* ИУС на основе *FMEA*– или *SFMEA*– таблиц, для которых обязательным является задание элемента t_f,

– *функциональной безопасности*, когда должна быть оценена критичность отказов с учетом как вероятности p_f, так и тяжести u_f *(FME(C)A* – или *SFME(C)A* – таблицы);

– *информационной безопасности*, когда учитываются внешние информационные воздействия $v(x)_f$ (в этом случае имеем *F(I)MEA*-таблицу [6]);

– *живучести*, когда необходимо учесть физические $v(ф)_f$, и информационные $v(x)_f$ воздействия и степень деградации системы, которая может быть

а)

Вероятность отказа	Тяжесть последствия отказа		
	Низкая	*Средняя*	*Высокая*
Низкая	5	4	3
Средняя	4	3	
Высокая	3		

б)

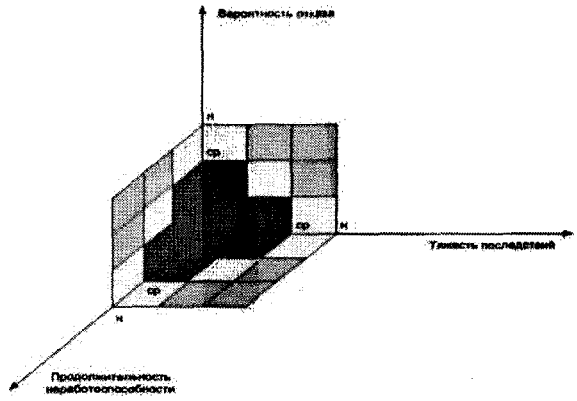

Рис. 2. Двух – (а) и трехмерная (б) матрица критичности

описана элементом u_f или его специальной частью $u_f(v)$.

Показатель $u_f(v)$, в отличие от традиционной оценки тяжести последствий, которая характеризует ее через уровень ущерба (в первую очередь, материального), ориентирован на оценку снижения качества функционирования системы – невозможности выполнения части функций или ухудшения соответствующих показателей качества. Описание процесса такого оценивания может быть проведено с использованием различных диаграмм деградации, так называемых *QD*-диаграмм [9].

Таким образом, разработанная модель позволяет оценить все свойства, составляющие *гарантоспособность* системы в соответствии с таксономической схемой, описанной в [7,8]. Если при этом ввести специальный столбец в таблицу – элемент m_f, который будет описывать возможные средства снижения рисков или парирования отказов (устойчивости к физическим и проектным дефектам, дефектам взаимодействия, обусловленным $v(\phi)_f$ и $v(x)_f$), то она будет представлять собой модель для оценки и обеспечения гарантоспособности системы:

$$FT=\langle v(\phi)_f, v(x)_f, e_f, c_f, r_f, p_f, u_f, u_f(v), t_f, m_f\rangle_{f=1}^{F}. \quad (5)$$

Данная модель включает все элементы, необходимые для проведения анализа гарантоспособности ИУС. Следует заметить, что введение средств m_f приводит к изменению показателей p_f, u_f, $u_f(v)$. Следовательно, после их введения эти показатели должны быть пересчитаны (переопределены).

Оцениваемые процессы

FMEA – подход используется для решения задач анализа и оценки характеристик *разрабатываемых или эксплуатируемых* систем. Он может применяться также для поддержки процессов *реинжиниринга* систем, который может предполагать функциональную, топологическую и надёжностную составляющие.

При *функциональном* реинжиниринге (расширении функций без изменения структуры схемы) в модели (5) могут корректироваться элементы r_f, p_f, u_f, t_f для части аппаратных средств и все элементы для некоторых компонент программных средств.

При *топологическом* (или структурном) реинжиниринге, когда выполняется добавление новых компонент или подсистем, осуществляется дополнение модели (5) путем внесения новых элементов F+1, F+2,....

При *надёжностном* реинжиниринге, связанном с повышением безотказности, готовности или других свойств, входящих в надёжность или гарантоспособность, могут изменяться элементы m_f, а также появляться дополнительные строки, соответствующие аппаратным и программным компонентам, поддерживающим функции отказоустойчивости. В этом случае должна быть проведена переоценка элементов p_f, u_f, t_f.

Методика и элементы информационной технологии оценки ИУС

На базе предложенных расширений *FME(C)A*- таблиц, методиках их получе-

ния и анализа может быть разработана *информационная технология* оценки и обеспечения гарантоспособности (безотказности, готовности, живучести и безопасности) ИУС при решении задач проектирования и реинжиниринга.

Её основными *операциями* при анализе гарантоспособности являются:

1) анализ структуры системы *IS* и представление её в виде множеств подсистем S_i, их аппаратных HW_{ij} и программных SW_{ik} компонент, значимых для проведения оценки соответствующих свойств системы;

2) определение множеств воздействий $v(x)_f$ и $v(ф)_f$, характерных для системы, подсистем и компонент (при оценке живучести и безопасности);

3) формирование элементов e_f, c_f, r_f списка FT_{IS} в соответствии с моделью (1);

4) определение вероятности p_f, тяжести u_f (и времени восстановления t_f при оценке готовности и живучести) для каждого из элементов списка FT_{IS} без учёта внешних воздействий и его уточнение с учётом воздействий $v(x)_f$ и $v(ф)_f$;

5) показатели p_f, u_f, t_f могут вычисляться в нечёткой (интервальной) шкале, задаваемой координатами значений

$$Mp_f(Mu_f,Mt_f)=$$
$$\langle p_{f1}(u_{f1},t_{f1}),\ldots,p_{fh}(u_{fh},t_{fh}),\ldots,p_{fh}(u_{fh},t_{fh})\rangle$$

6) или на основе точных количественных характеристик (интенсивности отказа), уровня потерь, интенсивности восстановления);

7) в первом случае выполняется построение матрицы (куба) критичности в пространстве

$$M_{\text{критичн}}=Mp_f\times Mu_f(\times Mt_f);$$

8) во втором – осуществляется переход к разработке деревьев отказов или Марковских моделей, позволяющих получить количественные значения показателей системы [4].

При разработке (реинжиниринге) системы *дополнительно* выполняются:

1) генерация множества вариантов программно-аппаратных средств

$$M_{mf}=\{m_{fa}\}_{a=1}^{zf}$$

снижения значений показателей p_f, u_f, t_f;

2) определение степени влияния каждого из вариантов $m_{fa}\in M_f$ на показатели p_f, u_f, t_f;

3) при нечёткой (интервальной) оценке варианты m_{fa} характеризуются по каждому из показателей парой значений - без использования и с использованием средств m_{fa} – вектором

$$\Delta PUT(m_{fa})=\{(p_{fa1},p_{fa2}),(u_{fa1},u_{fa2}),(t_{fa1},t_{fa2})\},$$

в котором значения $p_{fa1,2}$, $u_{fa1,2}$, $t_{fa1,2}$ принадлежат множествам M_{pf}, M_{uf}, M_{tf} соответственно;

4) выбор оптимального (рационального) подмножества вариантов $\Delta M_f^*\subset M_f$, которое обеспечит решение задачи в соответствии с заданными критериями (например, обеспечить приемлемый уровень критичности при минимальных затратах; уровень затрат определяется исходя из затрат d_{fa} на реализацию каждого из вариантов m_{fa}).

Информационная технология реализуется с использованием *программного комплекса*, включающего:

- утилиту поддержки разработки *FME(C)A*-таблиц на основе информации об ИУС,
- базу данных *FME(C)A*-таблиц,
- утилиту их анализа и оценки показателей гарантоспособности с использованием Марковских моделей, *FTA*-методик или других процедур,
- утилиту для поддержки оптимального выбора средств обеспечения требуемых характеристик надежности, живучести, безопасности при известных ограничениях.

Выводы

Комплексный характер предложенного развития *FME(C)A*-подхода состоит в том, что, в отличие от известных методов, учитываются различные свойства, составляющие гарантоспособность ИУС, различные факторы, влияющие на эти свойства и оцениваемые показатели.

Элементы предложенного метода использованы при анализе надежности университетской компьютерной сети [10] и распределенной ИУС для управления

нефтепроводом [11], анализе гарантоспособности сервис-ориентированных *web*-систем [5].

Сформулированные предложения по модернизации *FME(C)A*-таблиц и способам их использования позволяют перейти к разработке *детальных методик* оценки и обеспечения надежности, живучести и безопасности ИУС.

Следует отметить, что оценка тяжести последствий отказов их компонент должна осуществляться по схеме «сверху-вниз» (от системы к элементам), а оценка вероятности и времени восстановления - по схеме «снизу-вверх» (от элементов к системе).

Дальнейшие исследования могут быть связаны с решением *оптимизационных задач* в двух вариантах: как задач дискретной оптимизации при использовании матрицы (куба) критичности или задач оптимизации, когда показатели оцениваются с применением аппарата марковского анализа.

В практическом направлении следует разработать в полном объёме информационную технологию *поддержки принятия решений* при анализе и синтезе ИУС на основе комплексного *FME(C)A*-подхода.

Список литературы

1. *Черкесов Г.Н.* Надежность программно-аппаратных комплексов. – С.Пб.: Питер, 2005. – 479 с.

2. *Бегун В.В., Горбунов О.В., Каденко И.Н. и др.* Вероятностный анализ безопасности атомных станций. – К.: НТУУ «КПИ», 2000. – 328 с.

3. *Харченко В.С., Скляр В.В., Коноров Б.М. и др.* Оценка и обеспечение качества программных средств космических систем / Под ред. Харченко В.С., Конорева Б.М. – Харьков: НКАУ, Госцеткрачества, ХАИ, 2007. – 245 с.

4. *Харченко В.С., Ирадж Эльяси Комари.* Разработка марковских моделей надежности компьютерной сети информационно-управляющей системы с использованием FME(C)A – таблиц // Системи обробки інформації, №1 (45), 2007. – С. 56 – 60.

5. *Gorbenko A.V., Kharchenko V.S., Tarasyuk O.M., Furmanov A.A.* F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring, LNCS 4157, Rigorous Development of Complex Fault-Tolerant Systems / M. Butler et al. (eds.). – Springer, 2006. – P. 153 – 168.

6. *Hasan Sozer, Bedir Tekinerdogan, Mehmet Aksit.* Reliability Analysis at the Software Architecture Design Level using Enhanced Failure Modes and Effects Analysis Approach LNCS 4174, Architecturing Dependable Systems IV / R. de Lemos et al. (eds.). - Springer, 2007. – P.132 – 157.

7. *Kharchenko V.S., Sklyar V.V., Volkovoy A.V.* Multi-version Information Technologies and Development of Dependable Systems out of Undependable Components // Proceeding of IEEE DepCoS-RELCOMEX Conference, Szklarska Poreba, Poland, June 14-16, 2007. – P. 18 – 24.

8. *A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr.* Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Transactions on Dependable and Secure Computing, vol. 1, № 1, 2004. – P. 11 – 33.

9. *Kharchenko V.S.* The Probabilistic Assessment of Survivability and Safety of an Unmanned Control Systems with Multistage Degradation by Use of QD-diagrams //Proceeding of 5th International Conference on Probabilistic Safety Assessment and Management, Osaka, Japan, 27 November, 27 – December, 1, 2000, vol.1. – P. 525 – 531.

10. *Elyasi Komari Iraj, A. Gorbenko.* FME(C)A-Technique of Computer Network Reliability and Criticality Analysis. // Proceedings of IEEE East-West Design & Test Workshop, Conference, Sochi, Russia, September 15-19, 2006. – P. 202 – 205.

11. Telecommunication Alternatives and Best Choice for SCADA Networks. – National Iranian South Oil Company (NISOC), Project № 79217, 2007. – 38 p.