УДК 681.324

ИРАДЖ ЭЛЬЯСИ КОМАРИ, А.В. ГОРБЕНКО

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

АНАЛИЗ ГАРАНТОСПОСОБНОСТИ РАСПРЕДЕЛЕННЫХ ИУС НЕФТЕГАЗОВЫХ КОМПЛЕКСОВ С ИСПОЛЬЗОВАНИЕМ РАСШИРЕННЫХ FME(C)A-ТАБЛИЦ

Рассмотрены элементы метода анализа гарантоспособности распределенных информационно-управляющих систем (ИУС) для нефтегазовых инфраструктур. В его основе лежит выявление и анализ последствий различных отказов подсистем и компонентов (как программных, так и аппаратных), для систематизации которых предложено использовать иерархии FME(C)A-таблиц. Показан пример анализа ИУС нефтегазовой инфраструктуры компании NISOC.

гарантоспособность распределенных ИУС нефтегазовых инфраструктур, FME(C)A-анализ

Введение

В настоящее время проблема оценки и обеспечения гарантоспособности распределенных информационно-управляющих систем (РИУС) является наиболее актуальной для областей их критического применения, таких как химические и нефтегазовые производства, атомные электростанции, аэрокосмические комплексы и др.

При этом гарантоспособность является более общим свойством по сравнению с надежностью и охватывает, помимо безотказности и готовности, аспекты функциональной и информационной безопасности. Более подробно базовые понятия и таксономия гарантоспособности и её свойств применительно к системам различного типа, включая, в первую очередь, компьютерные сети, системы распределённой обработки информации, web-системы и др рассмотрены в [1].

Для оценки надежности (готовности) компьютерных систем широко применяются марковские модели. При этом, вместе с развитием и усложнением объекта анализа – распределенных информационно-управляющих систем, развиваются и сам математический аппарат, например, по пути создания многофрагментных макромоделей [2]. Однако при этом следует отметить, что в связи с расширением оцениваемых характеристик большое значение приобретает выявление характерных угроз и оценка степени их влияния на готовность системы и её компонент. Поэтому, наряду с традиционными математическим аппаратом методами оценки надежности, такими как марковские модели, все большую важность приобретают методы качественной оценки, такие как FTA [3, 4] и FME(C)A [5].

Цель статьи – разработка элементов метода анализа гарантоспособности распределенных ИУС с использованием модифицированной FME(C)A- технологии и иллюстрация возможности его применения для нефтогазовых инфраструктур.

Формализация и расширение FME(C)A-таблиц

Классическая FME(C)A-таблица FT является списком отказов, который может быть представлен множеством из F векторов (числом строк таблицы являются элементы системы и их отказы):

$$FT = < ef, cf, rf, pf, uf >_{f=1}^{F}, \quad (1)$$

где ef – отказавший элемент (причина отказа);

cf – вид отказа;

rf – последствие проявления отказа;

pf, uf – вероятность и тяжесть отказа соответственно, которые могут задаваться на нечёткой шкале (на-

пример, «высокая» - «средняя» - «низкая»).

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.

Детализация объекта 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 [4]. В [5] 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), подход к разработке которой может базироваться на парадигме «гарантоспособная система из негарантоспособных компонент» [6]. В этом случае от одиночной таблицы отказов FT, описываемой моделью (1), следует перейти к их иерархии FTIS, описываемой набором вложенных множеств компонент системы:

$$FTIS=\{FTS_k=\{FTHW_k=\{FTHW_{ki}\}, FTSW_k=\{FTSW_{kj}\}\}, \quad (2)$$

где FTS_k – модель (таблица) системы S_k, k=1..K (K – число систем (подсистем) инфраструктуры IS);

$FTHW_k$, $FTSW_k$ – модели (таблицы) для аппаратных и программных средств подсистемы Sk;

$FTHW_{ki}$, $FTSW_{kj}$ – модели (таблицы) i-той аппаратной и j-той программной компонент ($i=1..n_k$, $i=1..m_k$).

Применение FME(C)A для анализа характеристик гарантоспособности

FME(C)A – подход, который может быть использован для оценки различных характеристик гарантоспособности, в частности:

- безотказности ИУС, когда модель (1) может включать часть элементов, а именно ef, cf, rf, pf;
- готовности ИУС на основе FMEA- или SFMEA-таблиц, для которых обязательным является задание элемента tf;
- функциональной безопасности, когда должна быть оценена критичность отказов с учетом как вероятности pf, так и тяжести uf (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 описана элементом uf или его специальной частью uf (v).

Показатель uf (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.

Таким образом, разработанная модель позволяет оценить все свойства, составляющие гарантоспособность системы в соответствии с таксономической схе-

мой, описанной в [1]. Если при этом ввести специальный столбец в таблицу – элемент mf, который будет описывать возможные средства снижения рисков или парирования отказов (устойчивости к физическим и проектным дефектам, дефектам взаимодействия, обусловленным v(ф)f и v(x)f), то она будет представлять собой модель для оценки и обеспечения гарантоспособности системы:

$$FT = \langle v(ф)f,\ v(x)f,\ ef,\ cf,\ rf,\ pf,\ uf,\ uf(v),\ tf,\ mf \rangle_{f=1}^{F}.$$

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

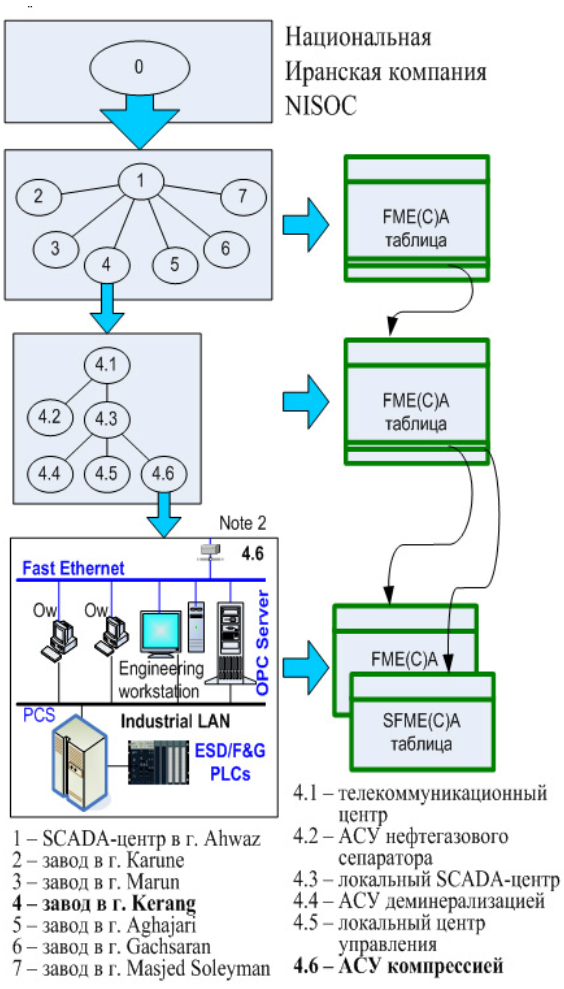

Рис. 1. Отображение иерархии оцениваемой системы на иерархию FME(C)A-таблиц

Анализ безопасности распределенных ИУС для нефтегазовых инфраструктур

Безопасность нефтегазовых и энергетических комплексов непосредственно зависит от совершенства применяемых сетевых и компьютерных технологий. Распределенные информационно управляющие системы реализуются посредством этих технологий, PLC-оборудования нижнего уровня и являются ядром инфраструктур. Отказы РИУС могут привести к серьезным авариям и материальным потерям. Для оценки готовности, функциональной и информационной безопасности применяются различные методы оценки, базирующиеся на аппарате марковских процессов, FMEA (SFMEA, IMEA) - и FTA-анализе, методах теории рисков и др.

Комплексная методика оценивания базируется на представлении исследуемых систем в виде иерархических структур, компоненты которых описываются стандартными табличными формами анализа видов и последствий отказов, вызванных различными факторами – дефектами технических средств (FMEA), проектными дефектами программных средств (SFMEA), внешними физическими и информационными воздействиями (IMEA). Далее, на основе этих таблиц в зависимости от особенностей применяемых сетевых технологий, организации обслуживания и ремонта оборудования, осуществляется переход к иерархии марковских моделей.

На рис. 1 приводится пример проведения такого анализа для компьютерной сети нефтегазовых коммуникаций и дистанционно-управляемого энергетического комплекса малой мощности Национальной Иранской южной нефтяной компании (National Iranian South Oil Company – NISOC) Инфраструктура NISOC содержит семь подразделений - РИУС. Структура одной из РИУС представлена на рис. 2. Она включает шесть подсистем (4.1-4.6, рис. 1), каждая из которых имеет свою структуру. Каждому из элементов поставлена в соответствие FME(C)A-таблица и фрагмент марковской модели.

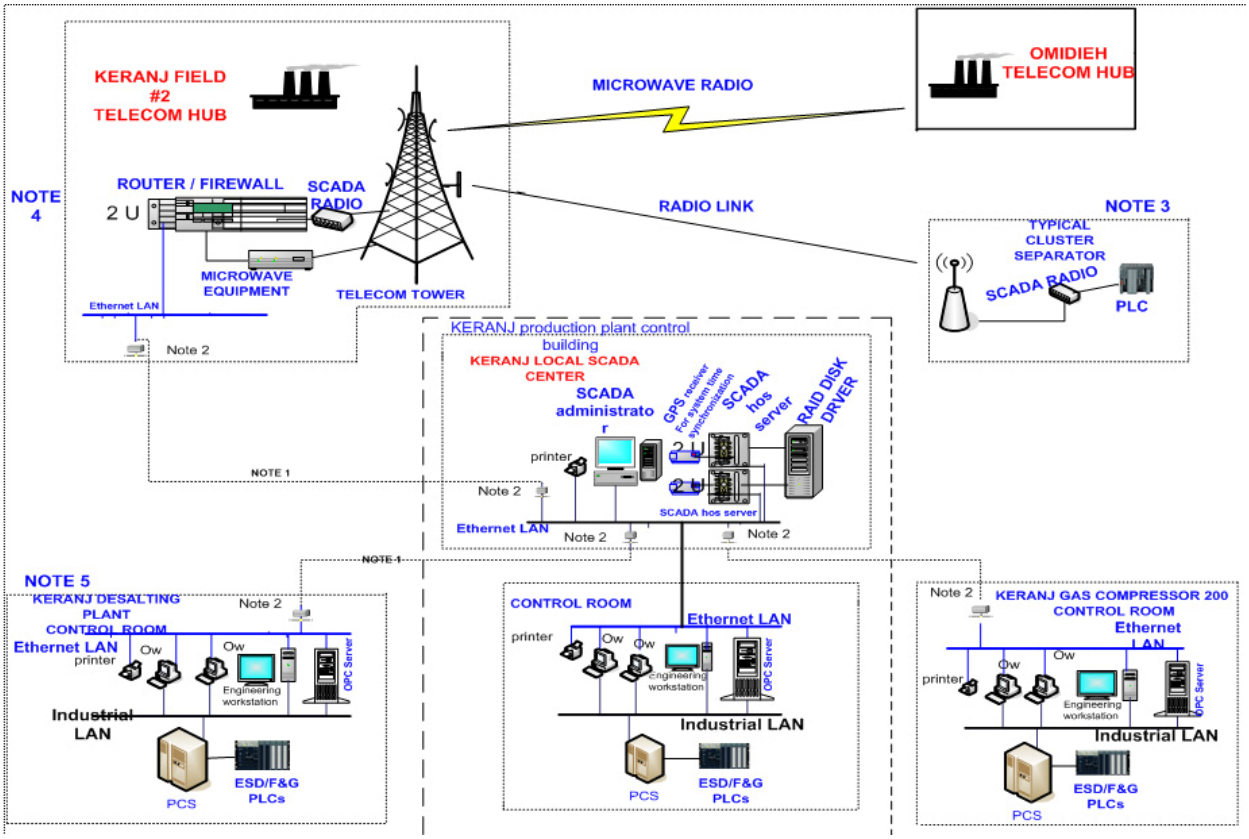

Рис. 2. Структура ИУС нефтеперерабатывающего завода в г. Kerang – одного из семи подразделений Национальной Иранской южной нефтяной компании

Представление РИУС иерархией FME(C)A-таблиц, а затем и многофрагментной марковской моделью позволяет осуществить анализ гарантоспособности. Данная методика поддерживается информационной технологией, которая может быть интегрирована со SCADA-системой [5].

Литература

1. Харченко В.С. Гарантоздатність комп'ютерних систем: проблеми, напрямки досліджень, результати // Радіоелектроннii комп'ютерні системи. – 2006. – № 5 (17). – С. 105-109.

2. Харченко В.С., Одарущенко О.Н., Одарущенко Е.Б.. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно- управляющих комплексов // Радіоелектронні і комп'ютерні системи. – 2006. – № 5 (17). – С. 45-52.

3. Keshtgary M., Jahangir A.H., Jayasumana A.P. Network Survivability Performance Evaluation using fault Trees. // Proc. 3rd IASTED Conference on Communication Computer Networks (CCN 2005), CA, USA, Oct. 2005. – P.158-163.

4. J. D. Andrews, and C. A. Ericson. Fault Tree and Markov Analysis Applied to various design complexities // Proc. 18th International System Safety Conference. – 2000.

5. Ирадж Эльяси Комари. Совершенствование методов и технологии оценки готовности и безопасности распределенных информационно-управляющих систем для нефтогазовых и энергетических инфраструктур // Тр. Міжн. науково-технічної конференція "Інтегровані комп'ютерні технології в машинободуванні ІКТМ-2007". – Х.: НАКУ «ХАІ», 2007. – С. 680.

Поступила в редакцию 22.02.2008

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Жуковского Н.Е. «ХАИ», Харьков.