УДК 681.324

ИРАДЖ ЭЛЬЯСИ КОМАРИ, А.В. ГОРБЕНКО

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

МЕТОД ОПТИМАЛЬНОГО ВЫБОРА СРЕДСТВ СНИЖЕНИЯ КРИТИЧНОСТИ ОТКАЗОВ ПО РЕЗУЛЬТАТАМ FME(C)A – АНАЛИЗА

В статье рассматривается метод обеспечение надежности и функциональной безопасности информационно-управляющих систем (ИУС) энергетики, и для каждого конкретного отказа формируется номенклатура методов и средств, направленных на снижение тяжести отказов, уменьшения как времени, затрачиваемого на восстановление после отказов, так и вероятности их возникновения с использованием многомерных матриц критичности.

Ключевые слова: *надежность и функциональная безопасность ИУС, снижение критичност отказов, FME(C)A-анализ.*

Введение

Обеспечение надежности и функциональной безопасности распределенных информационно-управляющих систем (РИУС) является наиболее актуальной для систем критического применения, таких как химические и нефтегазовые производства, атомные электростанции, аэрокосмические комплексы и др.[1].

По имеющимся данным каждый пятый отказ оборудования атомных электростанций или аварий обусловлен отказами ИУС [2].

При возникновении отказов на таких объектах последствия от реализации событий могут приводить к нарушению связности между различными подсистемами, потери работоспособности ИУС, значительным экономическим ущербам, различного уровня техногенным и экологическим катастрофам, фатальным последствиям для населения [3].

В известных работах [1, 4, 5] описываются различные аспекты, и представляется целесообразным использование всех возможностей новых информационных технологий для снижения рисков или снижения критичности отказов.

Поэтому, наряду с традиционными математическим аппаратом методами оценки надежности, такими как Марковские модели [6]. Все большую важность приобретают методы надежности и функциональной безопасности [7] и качественной оценки, такие как методы формализованной оценки, базирующиеся на анализе (FMEA) [8], критичности отказов - FME(C)A , построении деревьев отказов и событий – FTA [9, 7], и анализе аварийных ситуаций - HAZOP. [10, 11] , 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 [12].

Цель статьи – разработка методики снижения критичности отказов при минимизации затрат и выбора технологий обеспечения отказоустойчивости информационно-управляющих систем сложных технических комплексов.

1. Методы снижения критичности отказов (ИУС)

Для компьютеризированных систем существует достаточно большая номенклатура методов и средств, направленных на снижение критичности отказов, уменьшения как времени, затрачиваемого на восстановление после отказов, так и вероятности их возникновения. К последней категории традиционно относятся различные виды избыточности и средства резервирования.

Уменьшение времени восстановления информационно-управляющих систем возможно за счет внедрения средств диагностирования, а также автоматизации самих процедур ремонта и восстановления элементов системы (рис. 1).

Например, при организации компьютерной сети могут быть использованы дорогостоящие коммутаторы, имеющие в своем составе средства диагностики и автоматической реконфигурации структуры сети при возникновении отказов отдельных сегментов кабеля или сетевых устройств. Другим примером служит применение в компьютерной сети вместо статической (настраиваемой администратором) маршрутизации – динамиче-

скую, основанную на использовании протоколов маршрутизации, которые пересылают специальные диагностические сообщения о состоянии сети между маршритизаторами и служат для выбора или коррекции маршрута пересылки информационных пакетов.

Для снижения тяжести отказов применяются системотехнические методы, направленные на изменение архитектуры системы, её разбиение на подсистемы, а также внедрение специальных подсистем, предназначенных для недопущения катастрофических последствий отказов, как, например системы аварийной защиты реактора на атомных электростанциях.

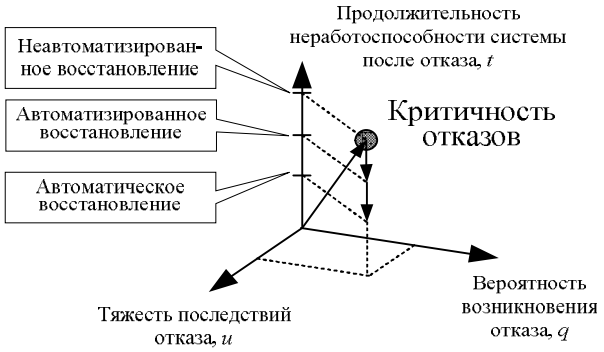

Рис. 1. Снижение времени неработоспособности компьютерной сети после отказа

Поскольку классическая методика оценки видов и последствий отказов FME(C)A предполагает качественную оценку критичности, то оценку степени эффективности методов и средств восстановления после отказов и обеспечения отказоустойчивости на первом этапе также можно выполнить в качественном виде. В этом случае можно допустить, что каждое средство обладает способностью уменьшения тяжести последствия отказа или вероятности его возникновения с некоторого начального уровня на некоторое дискретное значение.

Например, при таком качественном подходе к оцениванию можно сделать допущение о том, что однократное резервирование снижает вероятность возникновения некоторого отказа с уровня «высокий» до уровня «средний», или с уровня «средний» до уровня «низкий», а двухкратное – с уровня «высокий» сразу до уровня «низкий».

Для отказов, находящихся в ячейке матрицы критичности, непосредственно граничащей с диагональю критичности (см. рис. 2-а), перевод в зону некритических отказов возможен путем применения средств, переводящих на одну «ступеньку» или вниз или вправо. Для отказов, отстоящих от диагонали критичности на большее расстояние (см. рис. 2-б) необходимо комплексное применение средств, переводящих отказ вправо-вниз по матрице критичности на одну или несколько «ступенек».

Как видно из рисунка 2, если в случае (а) возможно минимум два варианта снижения критичности за счет снижения либо вероятности возникновения, либо тяжести последствий отказа, то в случае (б) таких вариантов становиться минимум четыре за счет комбинации различных методов и средств снижения того или иного аспекта критичности.

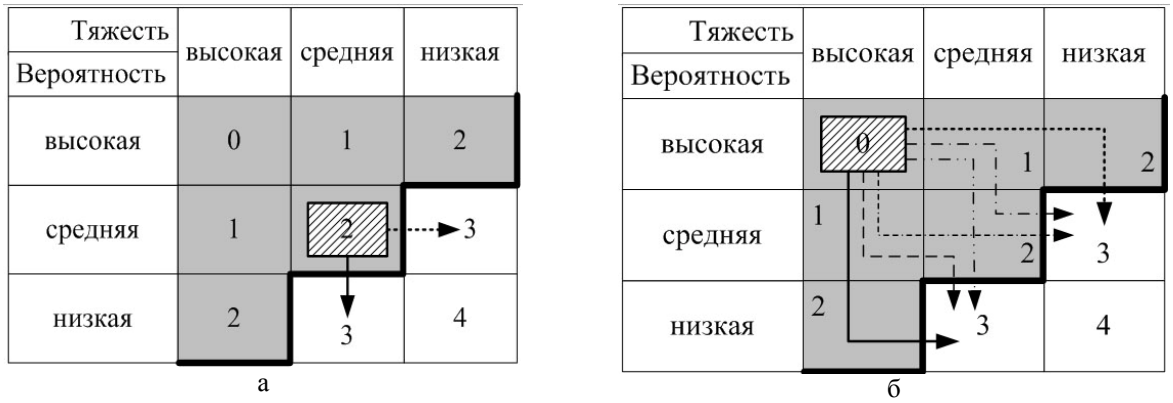

Рис. 2. Снижение критичности отказов

2. Оценка эффективности методов и средств снижения критичности отказов

Для оценки эффективности методов и средств снижения критичности отказов при качественном подходе предлагается каждому методу (средству) поставить в соответствие число ячеек, на которое отказ сдвигается в зону некритических отказов. Например, если некоторое средство позволяет снизить вероятность возникновения некоторого отказа с уровня «высокий» до уровня «средний», или с уровня «средний» до уровня «низкий», то его эффективность оценивается числом «1». а с уровня «высокий» до уровня «низкий» – числом «2».

Поскольку каждое средство может одновременно влиять на несколько характеристик критич-

ности (вероятность отказа, тяжесть последствий, время восстановления) то его можно описать множеством {ep, eh, et}, где ep – эффективность снижения вероятности возникновения отказа, eh – эффективность уменьшения тяжести последствий отказа, et – эффективность снижения времени восстановления. Причем, ep, eh, et = 0..2 для трехкатегорийной качественной шкалы оценивания. Суммарная эффективность является интегральной величиной:

$$e = ep + eh + et. \quad (б)$$

Очевидно, что доступные методы и средства снижения критичности отказов не являются полностью универсальными, а подходят для только одного или группы отказов. Соответствие доступных методов и средств восстановления после отказов и обеспечения отказоустойчивости может быть задано в виде матрицы, строками которой является множество отказов системы F, выявленных на первом этапе FMECA анализа, а столбцами – доступные средства и их эффективность снижения вероятности возникновения ep, уменьшения тяжести последствий eh и снижения времени восстановления et относительно каждого отказа, как это показано в табл. 1.

С учетом (1) таблица 1. может быть представлена в сокращенном виде, как это показано на примере табл. 2.3, которая содержит только интегральную эффективность методов и средств снижения критичности (повышения некритичности) относительно каждого отказа.

Таблица 1

Пример оценки эффективности методов и средств снижения критичности отказов

	Методы и средства снижения критичности отказов и их эффективность											
	m1			m2			mj			mn		
Отказ	ep1	eh1	et1	ep2	eh2	et2	epj	ehj	etj	epn	ehn	etn
f1	0	1	1	0	0	0	0	0	2	0	0	0
f2	1	0	0	0	0	0	0	0	1	0	1	1
fi	1	0	1	1	0	0	0	1	1	0	0	0
fm	0	0	0	1	0	1	0	0	0	1	0	0

Применение того или иного метода или средства для снижения критичности (повышения некритичности) отказов требует определенных затрат. Очевидно, что эти затраты будут зависеть от выбранного метода (средства) и собственно отказа, для снижения критичности которого этот метод (средство) применяется. Например, стоимость резервирования кабеля протяженностью 100 метров будет больше, чем 50-метрового кабеля, а стоимость резервирования волоконно-оптического кабеля будет выше стоимости резервирования электрического кабеля «витая пара» той же длинны. Стоимость применения того или иного метода (средства) снижения критичности (повышения некритичности) отказов может быть задана табличным методом, так же как и интегральная эффективность (табл. 2).

Таблица 2

Интегральная оценка эффективности и стоимости методов и средств снижения критичности отказов

	Стоимость и интегральная эффективность методов и средств снижения критичности отказов							
Отказ	m1		m2		mj		mn	
	e1	c1	e2	c2	ej	cj	en	cn
1	2		0		2		0	
2	1		0		1		2	
i	2		1		2		0	
m	0		2		0		1	

3.Задачи оптимального выбора

Задача оптимального выбора методов и средств снижения критичности (повышения некритичности) отказов может быть выполнена в двух постановках:

1) минимизация затрат на приобретение и внедрение методов и средств снижения критичности отказов при снижении уровня критичности (повышение некритичности) всех возможных отказов системы до некоторого заданного уровня (т.е. ниже диагонали критичности).

2) максимально возможное снижение критичности (повышение некритичности) отказов системы при заданных ограничениях на стоимость методов и средств, которые могут быть для этого использованы;

Первая задача выбора характерна для областей критического применения, к которым относятся информационно-управляющие системы нефтегазовых и энергетических комплексов. Формально она может быть сформулирована следующим образом:

$$f(x)=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{i,j}\,x_{i,j}=cx\to\min,\ x\in D, \qquad (7)$$

$$D=\left\{\begin{array}{l} x\in R^{mn}\mid\sum_{j=1}^{n}e_{i,j}\cdot x_{i,j}+d_i>CR,\\ i\in 1:m;\ x_{i,j}\in\{0;1\}\end{array}\right\}, \qquad (8)$$

где d_i – начальный уровень критичности (не критичности) i-го отказа;

C_R – число, задающее диагональ критичности (граничное значение критичности/некритичности);

$e_{i,j}$ – эффективность применения j-го метода (средства) по отношению к i-ому отказу.

$c_{i,j}$ – затраты на применение j-го метода (средства) для снижения критичности i-ого отказа.

Начальный уровень критичности (некритичности) i-го отказа задаётся некоторым числом, так же как и диагональ критичности и определяется ячейкой матрицы критичности, в которую данный отказ попадает в соответствии с качественной оценкой вероятности его возникновения, тяжести последствий и времени, требуемого на восстановление.

Искомые переменные $x_{i,j}$ определяются следующим образом:

$$x_{i,j}=\begin{cases}1,\ \text{åñëè}\ \ j-\text{é}\ \ \text{ì åòî ä ï ðèì åí ÿåòñÿ}\\ \text{äëÿ ñí èæåí èÿ êðèòè÷í î ñòè i – ãî\ î òêàçà;}\\ 0,\ \text{åñëè}\ \ j-\text{é}\ \ \text{ì åòî ä í å ï ðèì åí ÿåòñÿ}\\ \text{äëÿ ñí èæåí èÿ êðèòè÷í î ñòè i – ãî\ î òêàçà.}\end{cases}$$

Данная задача относится к классу комбинаторных задач, когда функция оптимизации задается на конечном множестве, элементами которого служат выборки из m x n элементов, т.е. n имеющихся методов (средств) снижения критичности, которые могут быть применены для каждого из m возможных отказов системы.

Однако, в ряде случаев значение искомых переменных xi,j может быть определено на множестве неотрицательных целых чисел $x_{i,j}\in Z+$. Это характерно, например, для случая, когда в качестве метода снижения критичности (вероятности возникновения) отказа применяется резервирование элементов.

В этом случае значение переменной xi,j задает кратность резерва. Соответственно, в таком случае в кратное число раз увеличивается и стоимость ci,j применения данного метода. Для некоторых случаев кратность резервирования может быть ограничена явным образом.

В такой постановке оптимизационная задача выбора методов и средств снижения критичности отказов относится к более широкому классу целочисленных задач линейного программирования. Тем не менее, она может быть сведена к подклассу комбинаторных задач. Для этого разная кратность резервирования должна быть представлена как отдельный метод со своей оценкой стоимости и эффективности, зависящей от кратности.

Как видно из (7) и (8), глобальная оптимизация целевой функции f(x) может быть сведена к поэтапной оптимизации, т.е. оптимальная минимизация затрат на применение методов и средств снижения критичности всех отказов системы является аддитивной целевой функцией, которой соответствует эффект такого решений для отдельного отказа (9).

$$f\left(x_{1,1},\ldots,x_{1,n},x_{2,1},\ldots,x_{2,n},x_{i,1},\ldots,x_{i,n},x_{m,1},\ldots,x_{m,n}\right)=\sum_{i=1}^{m}f_i\left(x_{i,j}\right). \qquad (9)$$

Для решения такой задачи целесообразно воспользоваться методом динамического программирования [13].

Для формулировки задачи снижения критичности отказов системы при заданных ограничениях на стоимость необходимо сформулировать целевую функцию. Для этого может быть использован средний арифметический показатель некритичности, который также дополнительно может быть взвешен с учетом важности каждого отказа.

Начальный обобщенный уровень некритичности системы определяется в соответствии с (10), а с учетом весов отказов – (11).

$$NCR=\frac{\sum_{i=1}^{m}d_i}{m}\ ; \qquad (10)$$

$$NCR=\sum_{i=1}^{m}a_i\,d_i\ ,\sum_{i=1}^{m}a_i=1\ . \qquad (11)$$

Тогда, задача снижения критичности отказов системы при заданных ограничениях на стоимость может быть задана в виде:

$$f(x)=\sum_{i=1}^{m}a_i\sum_{j=1}^{n}e_{i,j}x_{i,j}+d_i\rightarrow \rightarrow \max,\ \sum_{i=1}^{m}a_i=1,\ x\in D, \tag{12}$$

$$D=\left\{\begin{array}{l} x\in R^{mn}\mid \sum_{i=1}^{m}\sum_{j=1}^{n}c_{i,j}x_{i,j}\le C_{max};\\ x_{i,j}\in\{0;1\}\end{array}\right\}, \tag{13}$$

где d_i – начальный уровень (некритичности) i-го отказа;

C_{max} – максимально допустимая стоимость всех методов и средств, применяемых для снижения критичности отказов;

$e_{i,j}$ – эффективность применения j-го метода (средства) по отношению к i-ому отказу.

$ci_{,j}$ – затраты на применение j-го метода (средства) для снижения критичности i-ого отказа.

a_i – весовой коэффициент i-ого отказа.

Для решения поставленной задачи может быть использован один из методов дискретного программирования, например, метод ветвей и границ.

Выводы

Результаты совершенствования FMEA-анализа позвалили перейти к разработке метода обеспечения надежности и функциональной безопасности ИУС с использованием многомерных матриц критичности и процедур дискретной оптимизации.

Сформулированы и решены оптимизационные задачи как задачи дискретной оптимизации при использовании матрицы (куба) критичности в двух вариантах по критерию «критичность-затраты»:

– снижении критичности отказов до установленного диагональю критичности требуемого уровня при минимизации стоимостных затрат;

– максимальном снижении интегральной критичности отказов при заданных стоимостных ограничениях.

Литература

1. Ястребекий. М.А. Безопасность атоных станций: Информационные и управляющие истемы / М.А. Ястребекий, В.Н. Васильченко, С.В. Виноградская, В.М. Гольдрин, Ю.В. Розен, Л.И. Спектор, В.С. Харченко. – К.: Техніка, 2004. – 472с.

2. Бутова О.Н. Нарушения в работе АЭС, вызованные системой управления технологическими процессами энергоблока / О.Н. Бутова, В.В. Инюшев, Л.И. Спектор, М.А. Ястребенцкий // Ядерная и радиционая безопасность. - 2003. - Т. 7, № 4. - С. 54-63.

3. Хомініч В.С. Деякі питания кількісного аналізу безпеки функціонування потенційно небезпечних об,єктів / В.С . Хомініч, Б.О. Білецькии // Екологія і ресурси: зб. Наук. Праць Інституту проблем національної безпеки. - ІПНБ. - 2004 - № 10. – С. 67-72.

4. Харченко В.С. Новые информационные технологии и безопасность информационно-управляющих систем / В.С. Харченко, М.А. Ястребенцкий, В.В.Скляр // Ядерная и радиционая безопасность. - 2003. Т. 6 . - № 2. - с. 19-28.

5. Скляр В.В. Анализ безопасности и выбор технологий реализации информационно-управляющих систем АЭС: риск – ориентированный поход / В.В .Скляр, В.С. Харченко, А.А. Ушаков // Екологія і ресурси: зб. Наук. Праць Інституту проблем національної безпеки.- ІПНБ. - 2006. - № 13. – С. 39-64.

6. Харченко В.С. Комплексный анализ гарантоспособности информационно-управляющих систем и инфраструктур: FME(C)A-модели и информационная технология / Харченко В.С., Ирадж Эльяси Комари // Проблеми інформатизації та управління: зб. наук. праць НАУ. – Вип .1(23).- Київ, 2008. – С. 92-97.

7. Rausand M. System Reliability Theory; Models, Statistical Methods and Applications (Second Edition) / M. Rausand. - Wiley, New York, 2004.

8. Sozer H. Failure Modes and Effects Analysis Approach for Reliability Analysis at the Software Architecture Design Level /H. Sozer, B. Tekinerdogan, M. Aksit R. de Lemos et al. (Eds.): Architecting Dependable Systems IV, LNCS 4615. - 2007. Springer-Verlag Berlin Heidelberg. - pp. 409–433

9. IEC 1025-1990. Fault tree analysis (FTA) / Стандарт МЭК "Анализ дерева отказов", 1990 г.

10. Бегун В.В. Вероятностный анализ безопасности атомных станций / В.В Бегун, О.В. Горбунов, И.Н. Каденко. – К.: НТУУ «КПИ», 2000. - 328 с.

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

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

13. Зайченко Ю.П. Исследование операций. / Ю.П Зайченко. – К.: Вища школа. Головное изд-во, 1988. – 552 с.

Поступила в редакцию 15.02.2009

Рецензент – д-р техн. наук, проф., зав. каф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков, Украина.

МЕТОД ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗНИЖЕННЯ КРИТИЧНОСТІ ВІДМОВ ЗА РЕЗУЛЬТАТАМИ FME(C)A – АНАЛІЗУ

Іраджж Эльясі Комари, А.В. Горбенко

У статті розглядається метод забезпечення надійності і функціональної безпеки інформаційно-управляючих систем енергетики, що інформаційно-управляють, і для кожної конкретної відмови формується номенклатура методів і засобів, направлених на зниження тяжкості відмов, зменшення як часу, що витрачається на відновлення після відмов, так і вірогідності їх виникнення з використанням багатовимірних матриць критичності.

Ключевые слова: надійність і функціональна безпека ІУС, зниження критичності відмов, FME(C)A-аналіз.

METHOD OPTIMUM THE CHOICE OF MEANS REDUCTION OF CRITICALITY FAILURES BY RESULTS OF FME (C) A - ANALYSIS

Iraj Elyasi Komari, A.V.Gorbenko

In article the method ensuring of reliability and safety information-control systems (I&CS) power is considered, and for each concrete failure nomenclature of methods and means directed on decrease of consequences of failure, reduction of time spent on recovery after refusals, and probability of their occurrence is formed with use of multivariate matrixes criticality.

Keywords: reliability and safety (I&CS), decrease criticality failures, FME (C) A-analysis.

Ирадж Эльяси Комари – аспирант кафедры Компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail:I.elyasi@ csac.khai.edu.

Анатолий Викторович Горбенко – канд. техн. наук, ст. научн. сотрудник, доцент, кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского "ХАИ", Харьков, Украина, e-mail: A.Gorbenko@csac.khai.edu.