УДК 658.012.011

Е.В. БАБЕШКО, О.А. ИЛЬЯШЕНКО, В.С. ХАРЧЕНКО

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

МНОГОЭТАПНЫЙ АНАЛИЗ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Информационно-управляющие системы играют ключевую роль в обеспечении стабильной работы различных критических объектов и должны соответствовать требованиям национальных и международных нормативных документов. Для оценки и проверки указанных соответствий используется множество методов оценки надежности и безопасности. Преимущества и ограничения отдельных методов подробно описаны в литературе и закреплены в стандартах, однако далеко не всегда применение только одного метода является достаточным. В случае же совместного использования различных методов возникают вопросы совместимости данных между ними, наиболее рациональных этапов жизненного цикла для применения того или иного метода и т.д. Данная работа посвящена обсуждению согласованного применения методов анализа надежности и безопасности на различных этапах жизненного цикла информационно-управляющих систем.

Ключевые слова: *информационно-управляющая система, надежность, безопасность, FMECA, FTA, RBD.*

Введение

Информационно-управляющие системы (ИУС) являются по своей природе структурно-сложными техническими системами большой размерности. Для таких объектов можно выделить два основных направления по обеспечению надежности и безопасности:

– безаварийное (безотказное) функционирование ИУС с учетом имеющихся ресурсов;

– оперативное устранение последствий аварийных ситуаций в случае их возникновения и возобновление функционирования ИУС.

Для реализации этих двух направлений необходимы методы оценки надежности отдельных элементов и ИУС в целом.

В качестве таких методов в настоящее время широко используются FMECA, FTA, RBD, марковские модели, статистические методы и т.д.[1-3].

Каждый из методов имеет преимущества и ограничения. Проведенный анализ литературы [4-8] показал, что:

– методы оценки надежности элементов ИУС, основанные на статистических данных, в большинстве случаев используют только экспоненциальный закон распределения;

– методы оценки надежности и безопасности ИУС не позволяют выполнять анализ систем большой размерности за приемлемое время;

– отсутствует единый формат описания ИУС;

– возможности совместного использования методов анализа исследованы недостаточно;

– не существует универсального подхода, позволяющего выбрать наиболее подходящие методы анализа на различных этапах жизненного цикла системы.

В рамках данной статьи рассматриваются последние два аспекта. Цель статьи – обоснование возможностей совместного использования методов. В качестве основного метода взят анализ видов, последствий и критичности отказов (FMECA).

Взаимосвязь методов анализа надежности и безопасности ИУС

В качестве основного метода предлагается использовать анализ видов, последствий и критичности отказов (Failure Modes, Effects and Criticality Analysis, FMECA). Это связано, прежде всего, с его обязательным применением при лицензировании ИУС в соответствии со многими отраслевыми и общепромышленными стандартами, наглядностью и возможностью использования результатов анализа другими методами. Исходными данными для метода является техническая документация на ИУС (спецификация, перечень элементов, чертежи и т.д.).

Результаты FMECA могут быть использованы на следующих этапах при проведении анализа надежности с помощью дерева отказов (FTA, Fault Tree Analysis), блок-схем надежности (RBD, Reliability

Block Diagram), блок-схем безопасности (SBD, Safety Block Diagram), анализа отказов по общей причине (CCFA, Common Cause Failure Analysis), а также при построении марковских моделей (рис. 1).

Метод FTA направлен на выявление комбинаций отказов элементов системы, ошибок персонала и внешних (техногенных, природных) воздействий, приводящих к отказу системы в целом. Метод используется для анализа возможных причин возникновения отказа системы (качественная оценка) и расчета его вероятности (количественная оценка) на основе знания вероятностей исходных событий. Кроме того, некоторые события дерева отказов могут быть представлены с помощью марковских моделей (динамический FTA). Перечень исходных событий может быть получен по результатам предварительно проведенного FMECA.

Метод RBD заключается в графическом представлении системы в виде логических связей элементов (качественная оценка). При известных вероятностях безотказной работы элементов может быть рассчитана вероятность безотказной работы системы (количественная оценка). Блок-схему надежности часто создают непосредственно по функциональной блок схеме системы. Для уточнения блок-схемы надежности может быть использован перечень элементов, влияющих на работоспособность системы, полученный в результате проведенного предварительно FMECA.

Марковские модели (ММ) являются апробированным математическим аппаратом для моделирования и анализа надежности систем.

Проведенный предварительно FMECA- и (или) FTA-анализ позволяет определить дополнительные состояния системы и, следовательно, построить более точную модель. Результатом моделирования является граф состояний системы (качественная оценка). При известных интенсивностях (вероятностях) переходов между состояниями могут быть рассчитаны показатели безотказности и готовности системы (количественная оценка).

Результаты анализа отказов по общей причине CCFA могут быть использованы для уточнения блок-схемы надежности при последующем проведении RBD. Анализ CCFA может быть проведен как часть FMECA.

Результаты анализа

Результатом анализа надежности являются количественные либо качественные оценки. Некоторые методы позволяют получить как качественные, так и количественные результаты. Например, после построения блок-схемы надежности может быть выявлено влияние элемента ИУС на систему в целом (качественная оценка), при этом после проведения расчетов может быть получена вероятность безотказной работы ИУС (количественная оценка).

Информация о возможных результатах анализа надежности также представлена на рис. 1.

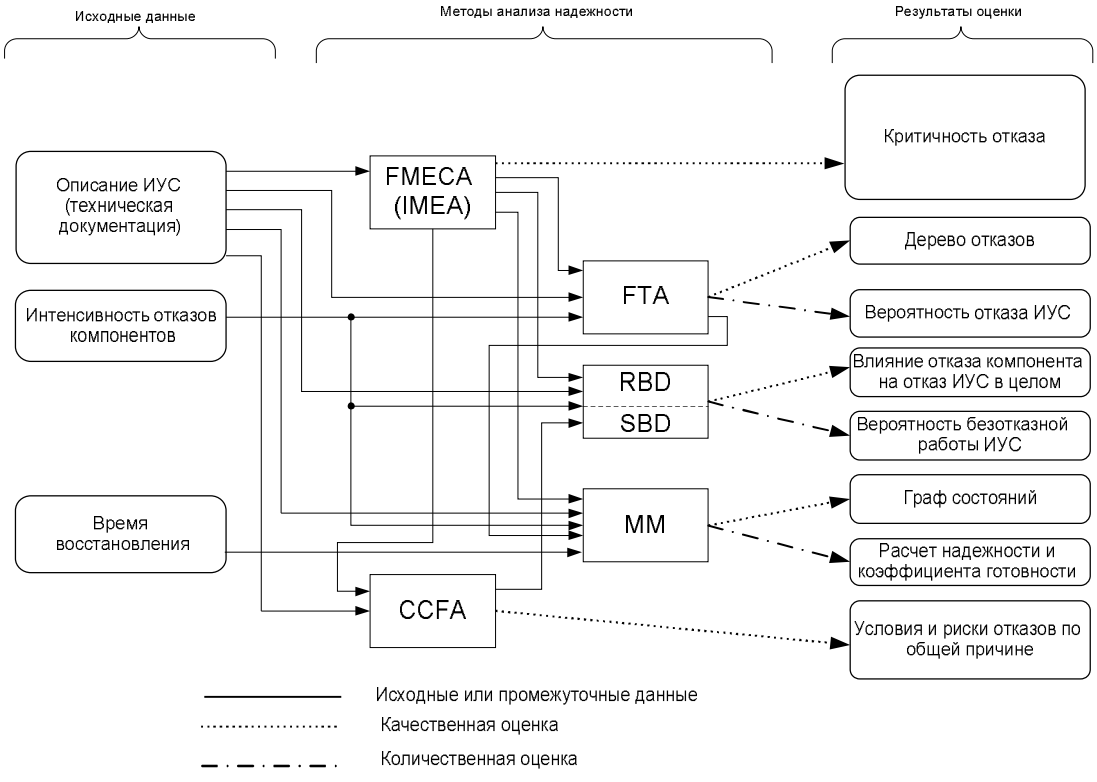

Рис. 1. Последовательное использование методов анализа надежности

Этапы анализа безопасности

В соответствии с требованиями международного стандарта МЭК 61508 [13], действия по управлению и оценке функциональной безопасности должны проводиться на всех этапах жизненного цикла. На рис. 3 представлен фрагмент жизненного цикла и методы, которые могут применяться на его этапах:

– этап «Определение всех областей применения». На данном этапе производится определение границ анализа опасностей и рисков, поэтому целесообразно применение методов FMECA и FTA;

– этап «Анализ источников риска и опасностей». Здесь используются результаты предыдущего FMECA- и FTA-анализов для более тщательной проработки данных методами RBD и CCFA;

– этап «Совокупные требования к безопасности». На данном этапе разрабатывается спецификация полных требований к безопасности. Удобным инструментом является метод, основанный на построении и анализе марковских моделей ИУС.

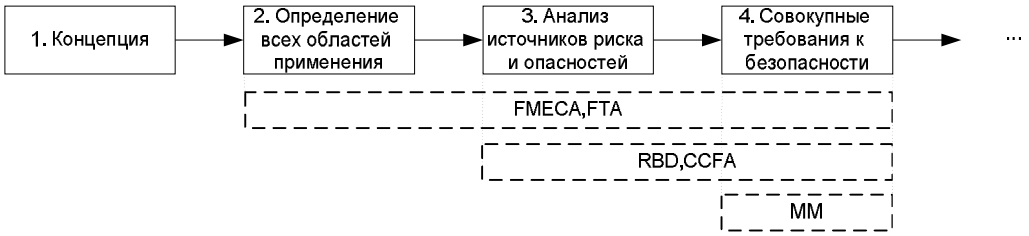

Рис. 3. Использование методов анализа на различных этапах жизненного цикла безопасности

Расширения методов анализа

К рассмотренным в работе методам анализа надежности существует множество модификаций (расширений), учитывающих особенности объекта анализа. Например, для анализа программного обеспечения существует метод SoftwareFMECA, для учета информационных воздействий – IntrusionMECA [14] и т.п.

В табл. 1 приведены различные виды дефектов ИУС и им поставлены в соответствие модификации метода FMECA.

Таблица 1

Разновидности FMECA

Вид события			Компоненты		Изменившееся состояние	Используемые методы анализа
Дефекты	Подвиды					
	Физические дефекты		Аппаратная часть		Техническое	FMECA
	Дефекты проектирования		Аппаратная часть		Техническое	FMECA
						DesignFMECA
			Программное обеспечение		Техническое	SoftwareFMECA
			Система в целом		Техническое, Информация	FMECA
						DesignFMECA
						ProcessFMECA
						HierarchFMECA
	Дефекты, вызванные внешним воздействием	Физическое воздействие	Аппаратная часть		Техническое	FMECA
		Информационное воздействие	Система		Техническое	IntrusionMECA
		Человеческий фактор	Физический	Аппаратная часть	Техническое	HumanMECA
			Информация	ПО	Техническое, Информация	
				Система	Техническое, Информация	

Информационная система анализа надежности ИУС

Одним из наиболее действенных способов снижения остроты проблем, перечисленных во введении, является создание системы управления надежностью ИУС, позволяющей выстраивать обоснованный баланс между затратами на содержание ИУС и рисками возникновения потерь по ее вине. В силу большого объема анализируемых данных и сложности математических расчетов, необходимых для качественного и своевременного анализа состояния ИУС, важнейшей составляющей управле-

ния надежностью является соответствующая информационная система.

Нами были сформулированы следующие задачи:

– разработка структуры и программная реализация системы модельно-алгоритмической поддержки многоэтапного анализа надежности сложных информационно-управляющих систем;

– применение системы при решении практических задач анализа и формирование эффективных по надежности архитектур информационно-управляющих систем.

Информационная система обеспечивает создание проектов, создание и заполнение FMECA-таблиц, проведение анализа надежности другими методами на основании FMECA-таблиц.

На рис. 2 показан пример построения блок-схемы надежности по данным из FMECA-таблицы.

№	Элемент	Идентификатор	Функция	Вид отказа	Причина	Последствия	Вероятность	Критичность	Примечание
1	Коммутатор	S01	Коммутация	Отсутствие связи	Отказ коммутатора	Невозможность	A	4	
2.1	Панель оператора	PAN01	HMI	Отсутствие HMI	Отказ панели	управления	B	2	
2.2	АРМ оператор	ARM01	HMI	Отсутствие HMI	Отказ АРМ	оператором	C	2	

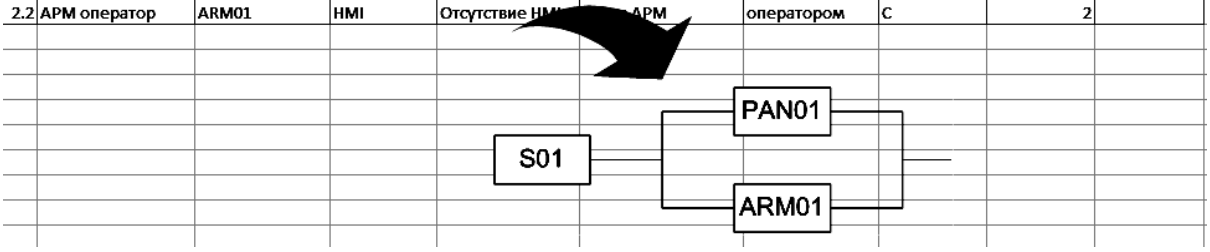

Рис. 2. Построение блок-схемы надежности по FMECA-таблице

Заключение

В статье были рассмотрены аспекты многоэтапного анализа надежности, включающего применение различных методов на различных этапах жизненного цикла. Показаны оценки, которые можно получить с помощью того или иного метода анализа. Сформулированы требования к информационной системе анализа надежности, основанной на FMECA в качестве основного метода. Дальнейшие исследования целесообразно направить на создание системы поддержки принятия решений на разных этапах жизненного цикла по всем составляющим надежности ИУС и связать рассмотренные методы с задачами управления надежностью по гибким стратегиям.

Рассмотренный подход к анализу надежности прошел апробацию в проектах научно-производственного предприятия «Радий» (Кировоград, Украина) и в настоящее время закреплен в стандарте предприятия [12].

Литература

1. Goble W.M. Control Systems Safety Evaluation and Reliability, 3rd ed. / W.M. Goble. – ISA Press, 2010. – 550 p.

2. Li H. Reliability Modeling Of Fault Tolerant Control Systems / H. Li, Q. Zhao., Z. Yang // International Journal of Applied Mathematics and Computer Science – 2007. – Vol. 17, No. 4. – P. 491–504.

3. Yu Y. Reliability Analysis for Continuous Operation System in Nuclear Power Plant / Y. Yu, J. Tong, R. Zhao, A. Zhang // ICRMS 2009. 8th International Conference on Reliability, Maintainability and Safety. – 2009. – P. 171-173.

4. Анализ существующих отечественных и зарубежных методов и методик проведения ВАБ и обоснование общей методологии ВАБ корабельных ЯЭУ. Научно-технический отчет. Российский научный центр "Курчатовский институт" / Институт ядерных реакторов. – М.: 2002. – 39 с.

5. Белов П.Г. Теоретические основы системной инженерии безопасности / П.Г. Белов. – К.: КМУГА,1997. – 426 с.

6. Bluvband Z. Failure analysis of FMEA / Z. Bluvband, P. Grabov // Reliability and Maintainability Symposium, 2009. RAMS 2009. Annual. – P. 344-347.

7. Исаев С.В. Такой FMEA нам не нужен! / С.В Исаев // Методы менеджмента качества. – 2008. – № 3. – С. 30-32.

8. Хан Дж. Дж. Анализ надежности с учетом видов отказов: полезный способ оценки и повышения надежности / Дж. Дж. Хан, Н. Доганавский, У.К. Мир // Методы менеджмента качества. – 2009. – № 6.

9. ДСТУ 2860-94. Надійність техніки. – К.: Держстандарт України, 1994. – 36 с.

10. Надежность технических систем и техногенный риск / под ред. М.И. Фалеева. – М., 2002. – 368 с.

11. Рябинин И.А. Надежность и безопасность сложных систем. СПб.: Политехника, 2000. – 248 с.

12. СТП 66-2009. Анализ надежности. Метод анализа видов, последствий и критичности отказов (FMECA). – Кировоград: НПП «Радий», 2009. – 29 с.

13. ГОСТ Р МЭК 61508-1 2007 – Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 1 – М., 2008 – 50 с.

14. Babeshko E. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring / E. Babeshko, A. Gorbenko, V. Kharchenko // Proceeding of IEEE DepCoS-RELCOMEX Conference, June 26-28. – Szklarska Poreba, Poland, 2008. – P. 309-315.

Поступила в редакцию 15.02.2010

Рецензент: д-р техн. наук, проф., зав. кафедрой производства радиоэлектронных систем летательных аппаратов В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

БАГАТОЕТАПНИЙ АНАЛІЗ НАДІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ

Є.В. Бабешко, О.О. Ілляшенко, В.С. Харченко

Інформаційно-керуючі системи грають ключову роль в забезпеченні стабільної роботи різних критичних об'єктів і повинні відповідати вимогам національних і міжнародних нормативних документів. Для оцінки і перевірки зазначених відповідностей використовується безліч методів оцінки надійності та безпеки. Переваги та обмеження окремих методів докладно описані в літературі і закріплені в стандартах, проте далеко не завжди застосування тільки одного методу є достатнім. У разі ж спільного використання різних методів виникають питання сумісності даних між ними, найбільш оптимальних етапів життєвого циклу для застосування того чи іншого методу і т.д. Дана робота присвячена обговоренню застосування методів аналізу надійності і безпеки на різних етапах життєвого циклу інформаційно-керуючих систем.

Ключові слова: інформаційно-керуюча система, надійність, безпека, FMECA, FTA, RBD.

MULTISTAGE RELIABILITY AND SAFETY ANALYSIS OF INFORMATION AND CONTROL SYSTEMS

E.V. Babeshko, O.O. Illiashenko, V.S. Kharchenko

Information & control systems play a key role in ensuring of stable work of various critical objects and should correspond to requirements of national and international standard documents. For assessment and check of the specified conformity the set of methods of reliability and safety estimation is used. Advantages and restrictions of separate methods are described in the literature in detail and fixed in standards, however usage of one method is not usually enough. In a case of various methods usage there questions of data compatibility between them, the questions of choosing of the most rational stages of life cycle for use of one or another method etc. This work is dedicated to discussion of the coordinated application of reliability and safety analysis methods at various stages of information & control systems life cycle.

Keywords: information and control system, reliability, safety, FMECA, FTA, RBD.

Бабешко Евгений Васильевич – аспирант, ассистент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: E.Babeshko@csac.khai.edu.

Ильяшенко Олег Александрович – студент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: illiashenko_oleg@hotmail.co.uk.

Харченко Вячеслав Сергеевич – д-р техн. наук, проф., зав. кафедрой компьютерных систем и сетей, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: V.Kharchenko@khai.edu.