УДК 658.012.011

Е.В. БАБЕШКО, В.С. ХАРЧЕНКО

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

ВОЗМОЖНОСТИ СОВМЕСТНОГО ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ МЕТОДОВ АНАЛИЗА ОТКАЗОВ СИСТЕМ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ

В статье проанализированы существующие методы анализа отказов, применяющиеся при разработке систем, важных для безопасности. Показаны их достоинства и недостатки, предложены критерии, по которым можно произвести сравнение методов, выполнена классификация. В заключение исследованы взаимосвязи между различными методами анализа отказов и варианты их совместного использования, а также сформулированы рекомендации по выбору методов. При проведении анализа надежности сложных или многофункциональных систем связи для достижения наилучшего результата необходимо применение нескольких методов анализа.

Ключевые слова: *отказ, риск, FMEA, FTA, HAZOP, RBD.*

Введение

Анализ отказов представляет собой сбор и исследование информации об отказах системы в целом либо элементов системы. Целями данного анализа являются определение причин отказов, предотвращение их появления в будущем либо сведение негативных последствий к минимуму, а также проведение оценок для получения информации о надежности системы и поддержания ее на требуемом уровне. Задача анализа отказов является частью более общей задачи оценки надежности и безопасности сложных систем. В настоящее время при анализе отказов применяются качественные, количественные и комбинированные методы исследования [1 – 2].

Большинство методов основывается на проведении опросов экспертов, применении численных методов, экспериментальных исследованиях, методах теории вероятности и математической статистики.

Наиболее распространенными методами анализа отказов являются анализ видов и последствий отказов FMEA, анализ дерева отказов FTA, исследование опасности и работоспособности HAZOP, анализ структурной схемы надежности RBD, статистические методы и т.д. Большинство методов определены международными и государственными стандартами [3 – 7], а также подробно описаны в литературе [8 – 12].

В данной работе предпринята попытка систематизировать существующие методы, проанализировать взаимосвязи и потоки данных между ними, а также сформировать рекомендации по набору методов для наиболее полного и достоверного анализа отказов сложных систем.

1. Основные этапы анализа отказов

В общем виде процедура анализа отказов представлена на рис. 1. На первом этапе проводится выявление опасных ситуаций и отказов, которые могут к ним привести.

На этапе исследования проводится построение моделей и их анализ. Выходной информацией, как правило, являются значения вероятности, критичности и обнаруживаемости отказов, однако возможен и расчет других параметров.

В заключение формируются предложения по внесению изменений в проект системы, предназначенных для предотвращения отказов либо выполнения соответствующих действий при их возникновении и обнаружении, т.н. корректировочные мероприятия.

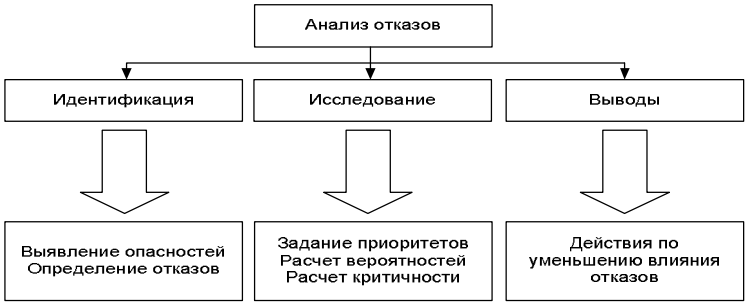

Рис. 1. Процедура анализа отказов

После проведения корректировочных мероприятий выполняется пересчет параметров.

Если не удалось добиться требуемых значений, разрабатываются дополнительные корректирующие мероприятия и повторяются предыдущие этапы.

На практике все этапы методов реализуются группой специалистов, причем, как правило, различного профиля.

2. Классификация методов анализа отказов

Проведем классификацию существующих методов анализа отказов. Сложность данной работы состоит в том, что изначально методы разрабатывались для различных целей и различных областей применения, а результаты методов часто трудно сравнимы между собой.

Рис. 2. Критерии сравнения методов

Для проведения классификации методов были выделены следующие критерии (рис. 2):

– тип анализа. По данному критерию выделяем количественный и качественный анализ, а также их комбинации. В табл. 1 приведены результаты, которые могут быть получены с помощью различных типов анализа различными методами.

– объект анализа (система, подсистема, элемент и т.п.);

– способ анализа – выделяем нисходящий (дедуктивный) и восходящий (индуктивный) способы;

– анализируемые классы отказов (единичные отказы либо комбинации отказов);

– этап применения – эффективность применения методов на различных этапах жизненного цикла системы может существенно различаться (рис. 3);

– наличие модификаций, которое косвенно говорит о простоте расширяемости метода. Наибольшее число модификаций у метода FMEA. Среди них анализ уязвимостей системы (IMEA) [13], анализ программного обеспечения (SFMEA) [14] и т.д.

Сравнение методов приведено в табл. 2.

Таблица 1

Методы анализа отказов и их типы

Метод	**Качественный анализ**	**Количественный анализ**
FTA	Анализ комбинации отказов	Вычисление показателей безотказности
RBD	Анализ вариантов работоспособности	Вычисление показателей безотказности и комплексных показателей надежности системы
FMEA	Анализ воздействия отказов	Вычисление критичности отказов системы
HAZOP	Анализ причин и последствий отклонений, вызванных отказами	Не применим
Статистические методы	Анализ воздействия отказов	Определение количественных оценок показателей безотказности

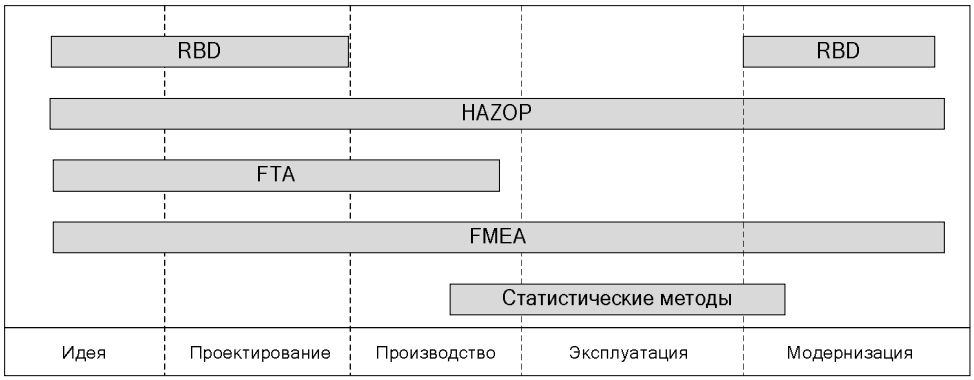

Рис. 3. Методы оценки надежности на различных этапа жизненного цикла

Таблица 2

Методы анализа отказов

	Исходные данные	**Кем выполняется**	**Достоинства метода**	**Недостатки метода**	**Область применения**	**Выходной результат**
FTA	информация о структуре и функциях системы	специалисты в области надежности	обеспечивает более глубокий анализ причин рисков	результаты оценки не формализованы	идентификация опасностей, инструмент для оценки вероятностей или частот отказов	дерево отказов, количественная оценка (при наличии исходной информации о надежности)
			высокая наглядность представления результатов	метод требует значительных затрат средств и времени		
			возможность выполнять как качественный, так и количественный анализ	только два состояния системы: рабочее и отказавшее		
			показывает в явном виде ненадежные места системы	описывает систему в определенный момент времени (обычно в установившемся режиме)		
RBD	информация о структуре системы и функциях	специалисты в области надежности	простота и наглядность	не различаются причины отказов	данные для дальнейших исследований	структурная схема надежности
FMEA/ FMECA	информация о структуре и функциях системы	группа специалистов различного профиля	рассматривается каждый компонент системы, позволяет проводить одновременно качественную и количественную оценки	избыточность, исключение из рассмотрения восстановительно-ремонтных действий, отсутствие анализа комбинаций отказов	исходные данные для FTA	таблица причин и последствий отказов, матрица критичности
AZOP	проектная документация (чертежи, руководства и т.д.)	группа специалистов различного профиля (от 4 до 7 человек)	систематический, упорядоченный и документированный подход	достаточно трудоемкий метод, требует больших трудозатрат	оценка рисков выхода из строя оборудования, часто используют на этапе проектирования	выявленные опасности и проблемы работоспособности, рекомендации для их обнаружения и/или уменьшения
Статистические методы	статистические данные об отказах	отдел статистики	позволяют получать результаты даже в тех случаях, когда не известна аналитическая связь между параметрами системы и результатом ее функционирования	не всегда есть достаточное время для сбора статистической информации	статистический анализ отказов	статистическая информация об отказах элементов системы
				результаты достоверны лишь с определенной вероятностью, задаваемой исследователями перед началом обработки статистических данных		

3. Совместное использование методов анализа отказов

Существуют методики, объединяющие в себе элементы различных методов [15]. Совместное использование методов позволяет решать более широкий класс задач и получать более достоверные результаты. Например, слабые места одного метода можно «закрыть» результатами другого.

Таблица 3

Сравнение особенностей FMEA и FTA

FMEA	FTA
Индуктивный (снизу вверх)	Дедуктивный (сверху вниз)
Определяет все возможные варианты отказов и их эффекты на систему	По отказу системы определяет возможные причины
Фокусируется на частях системы, которые могут привести к отказу	Фокусируется на системе в целом

Рассмотрим особенности методов FMEA и FTA. Из табл. 3 видно, что методы могут эффективно дополнять друг друга.

Практическим примером объединения FMEA и FTA может служить Bouncing Failure Analysis (BFA), представляющий собой комбинацию табличного и графического анализа [16].

В работе [17], выполненной специалистами компании Motorola, приводится пример объединенной методике анализа отказов, основанной на HAZOP и FMEA. Делается вывод, что такая связка значительно эффективнее использования методов по отдельности.

На рис. 4 представлены взаимосвязи методов. Каждый из них, основываясь на исходной информации о системе, позволяет получить результирующую оценку. Однако некоторые методы будут гораздо эффективнее, если они базируются на результатах других методов. Например, результаты FTA и RBD будут более точными, если уже известна информация о возможных отказах и их последствиях.

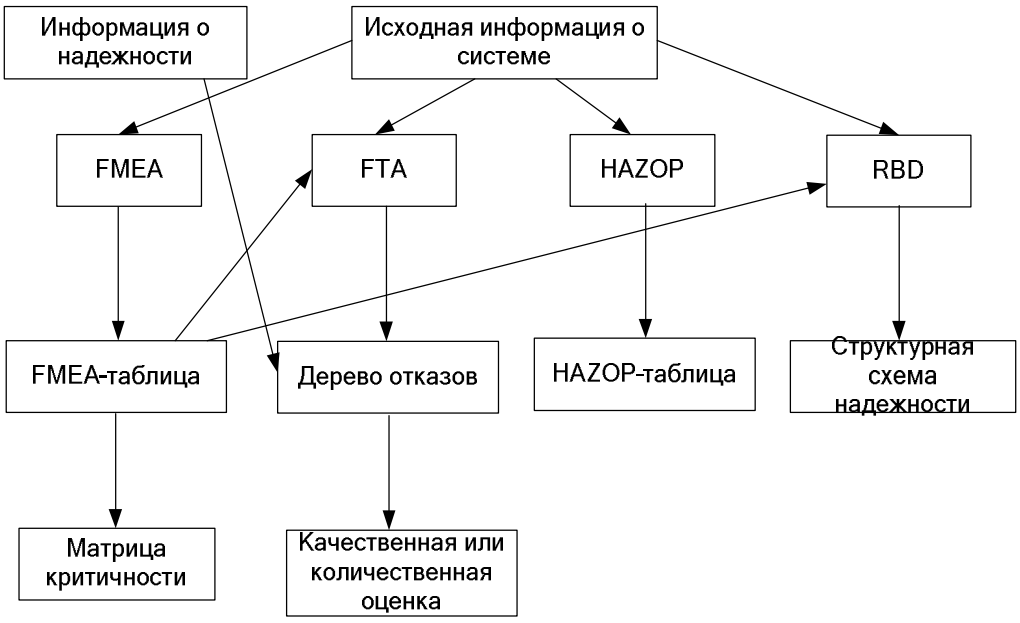

Рис. 4. Взаимосвязи методов

Заключение

Проведенное исследование показало, что в настоящее время существует множество различных методов анализов отказов.

Большинство из них основано на принципе разделения системы на подсистемы, элементы и т.д. и их последующем анализе. Данный принцип имеет ряд преимуществ, среди которых упрощение анализа, возможность выявления большего количества возможных отказов и т.п.

Однако в данном случае отказы рассматриваются как отказы отдельных элементов, а не отказы всей системы. Кроме того, не отслеживается взаимодействие различных частей системы между собой и не учитываются внешние воздействия.

Выбор метода должен осуществляться индивидуально для каждой системы и, по возможности, должен быть сделан на ранних этапах разработки и исследован на применимость.

При проведении анализа надежности сложных или многофункциональных систем связи для достижения наилучшего результата необходимо применение нескольких методов анализа.

Литература

1. Горский В.Г. Научно-методические аспекты анализа аварийного риска / В.Г. Горский, Г.А. Моткин, В.А. Петрунин, Г.Ф. Терещенко, А.А. Шаталова. – М.: Экономика и информатика, 2002. – 260 с.

2. Макдональд Д. Промышленная безопасность, оценка риска и системы аварийного останова / Д. Макдональд – М., 2007. – 409 с.

3. IEC 60812 Ed. 2.0 b:2006. Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

4. BS 5760-5:1991. Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis (FMEA and FMECA).

5. IEC 61025:2007. Fault tree analysis (FTA).

6. IEC 61882:2001. Hazard and operability studies (HAZOP studies) – Application guide.

7. BS EN 61078:2006. Analysis techniques for dependability – Reliability block diagram and Boolean methods.

8. Clifton A. Ericson II. Hazard Analysis Techniques for System Safety / Clifton A. Ericson II. – John Wiley & Sons, 2005. – 528 p.

9. Redmill F. System Safety: HAZOP and software HAZOP / F. Redmill, M. Chudleigh, J. Catmur. – Chichester, 1999.

10. Hyatt N. Guidelines for Process Hazards Analysis (PHA, HAZOP). Hazards Identification, and Risk Analysis / N. Hyatt. – CRC Press, 2004.

11. Анализ видов и последствий потенциальных отказов. FMEA. Ссылочное руководство. – Н.Новгород, 2006. – 86 с.

12. Rausand M. System Reliability Theory: Models, Statistical Methods, and Applications, Second Edition / M. Rausand, A. Høyland. – John Wiley & Sons, 2004. – 636 p.

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

14. Reifer D.J. Software Failure Modes and Effects Analysis / D.J. Reifer // IEEE Transactions on Reliability. – 2001. – R-28(3). – P. 247-249.

15. McDonald M. The Practical Guide to Defect Prevention / M. McDonald, R. Musson, R. Smith. – Microsoft Press, 2008. – 480 p.

16. Bluvband Z. Bouncing failure analysis (BFA): the unified FTA-FMEA methodology / Z. Bluvband, R. Polak, P. Grabov // Reliability and Maintainability Symposium. Proceedings. Annual. – 2005. – P. 463-467.

17. Trammell S.R. Using a modified HAZOP/ FMEA methodology for assessing system risk' / S.R Trammell, B.J. Davis // Engineering Management for Applied Technology. – 2001. – P. 47-53.

Поступила в редакцию 16.02.2009

Рецензент: д-р техн. наук, проф., зав. кафедрой, декан факультета В.М. Илюшко, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков, Украина.

МОЖЛИВОСТІ СУМІСНОГО ВИКОРИСТАННЯ СУЧАСНИХ МЕТОДІВ АНАЛІЗУ ВІДМОВ СИСТЕМ, ВАЖЛИВИХ ДО БЕЗПЕКИ

Є.В. Бабешко, В.С. Харченко

В статті проаналізовані існуючі методи аналізу відмов, що застосовуються при розробці систем, важливих до безпеки. Наведені їх позитивні та негативні якості, запропоновані критерії, за якими можливо виконати порівняння методів, наведена класифікація. Досліджені взаємозв'язки між різними методами та варіанти їх сумісного використання, також сформульовані рекомендації з вибору методів.

Ключові слова: відмова, риск, FMEA, FTA, HAZOP, RBD.

POSSIBILITIES OF COMBINED USAGE OF FAILURE ANALYSIS METHODS FOR SAFETY-CRITICAL SYSTEMS

E.V. Babeshko, V.S. Kharchenko

This article addresses existing failure analysis methods. Pros and cons of these methods are given. Comparison criterions are proposed and the classification is performed. Interconnections between different methods and variants of their combined usage are examined. In conclusion recommendations of method selection are formulated.

Keywords: failure, risk, FMEA, FTA, HAZOP, RBD.

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

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