УДК 621.3

О. А. ИЛЬЯШЕНКО, В. С. ХАРЧЕНКО, Я. А.ЧУЙКОВ

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

ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМ НА FPGA С ИСПОЛЬЗОВАНИЕМ XMECA ДЛЯ V-МОДЕЛИ ЖИЗНЕННОГО ЦИКЛА

В статье проведен анализ достоинств и недостатков метода XMECA для оценки безопасности разных компонент и видов отказов (X) системы, его. Исследованы особенности применения XMECA на основных этапах жизненного цикла системы. Проведен анализ V-модели жизненного цикла разработки систем на базе программируемой логики. Предложен комплекс рекомендаций по применению XMECA для анализа процессно-продуктных аномалий (отказов, несоответствий и т.д.) для V-модели жизненного цикла разработки систем на базе FPGA. Эти рекомендации адресованы различным элементам V-модели, модифицированной с учетом требований по функциональной и информационной безопасности

Ключевые слова: *FMECA, жизненный цикл, риски, отказы, функциональная безопасность, информационная безопасность*

Введение

Для того чтобы достичь необходимого уровня надежности, функциональной и информационной безопасности информационно-управляющих систем (далее систем) необходимо проводить их оценивание на всех этапах жизненного цикла, начиная от анализа концепции и заканчивая обслуживанием и выводом из эксплуатации.

При разработке систем критического применения, в том числе на базе Field Programmable Gate Arrays (FPGA), одним из обязательных методов является анализ видов, последствий и критичности отказов Failure Modes, Effects and Criticality Analysis (FMECA) [1]. В работах [2-3], указывается на необходимость использования различных типов XMECA (где X может указывать на разные виды отказов и анализируемых компонентов-продуктов и процессов) и аспекты их применения для оценки безопасности и рисков систем. Особенности разработки и адаптации метода XMECA для анализа безопасности систем на FPGA исследованы в [4, 5]. В частности, в [5] анализируется опыт применения модифицированной процедуры FMEDA оценки безопасности модулей на основе FPGA для платформы RadICS и использования результатов такого анализа для реализации метода засева дефектов при валидации. Однако, в известных работах не осуществляется привязка других вариантов XMECA к процессам жизненного цикла систем на FPGA и их комплексирования в единую методологию, которая бы позволила оценить риски и возможный ущерб, вызванный потенциальными несоответствиями продуктов и процессов на ранних стадиях создания систем.

Целью статьи является анализ вариантов XME(C)A и обоснование рекомендаций по их сквозному применению на разных этапах жизненного цикла разработки систем на FPGA.

Анализ достоинств и недостатков FMECA

Главной особенностью использования основного вида XFMEA – FMECA, в отличии от методов анализа дерева отказов (Fault Tree Analysis), структурной схемы надежности (Reliability Block Diagram, RBD), исследования опасности и работоспособности (HAZard and OPerability study, HAZOP), является итеративное использование на всех этапах жизненного цикла разработки.

Следует выделить основные группы объектов, которым может быть нанесен ущерб впоследствии отказов [6-7]: персонал, население, материальные объекты (оборудование, сооружения), окружающая среда.

Относительная величина критичности (Risk Priority Number, RPN) используется для определения приоритетности выполнения мероприятий нацеленных на ликвидацию или снижение последствий отказов. RPN рассчитывается по формуле:

$$\mathrm{RPN} = \mathrm{S} \times \mathrm{O} \times \mathrm{D}, \qquad (1)$$

где S (Severity, степень тяжести) – величина тяжести последствий, т.е. степени воздействия отказа на систему в целом (величина безразмерная, может нормироваться);

O (Occurrence, возникновение) – вероятность

возникновения отказа для определенного временного периода (величина может определяться рангом, а не точным значением вероятности возникновения отказа);

D (Detection, обнаружение) – оценка возможности выявить и ликвидировать отказ до возникновения последствий для системы; чем больше вероятность скрытого отказа, тем больше значение D [7, 8].

Результаты анализа предоставляются в таблице с перечислением элементов системы, видов и причин отказов, частоты, последствий, критичности, средства выявления и рекомендаций по уменьшению критичности. Это способствует достижению требуемых характеристик безопасности систем согласно требованиям, а также предупреждению возникновения и ослаблению тяжести отказов.

Основные преимущества использования FMECA [9]:

- снижение трудозатрат и стоимости разработки на различных этапах жизненного цикла благодаря систематизации анализа и уменьшения потерь на последующих этапах, связанных с устранением или предупреждением отказов;

- обмен информацией между членами команды при анализе обеспечивает обучение и повышение квалификации сотрудников, а также улучшение качества последующих проектов.

К недостаткам использования FMECA можно отнести высокие требования к экспертам, формирование большего объема данных, неполная формализация данных об отказах, причинах, последствиях, нечеткое определение вероятности возникновений и критичности отказов [10].

Особенности применения XMECA на различных этапах ЖЦ

XMECA реализуется командой, которая, как правило, состоит из нескольких экспертов-инженеров, проводящих анализ системы (процесса), которые проводят «мозговой штурм». Результат напрямую зависит от уровня подготовки и профессионального опыта задействованных специалистов [11].

Классификация методик XME(C)A представлена в таблице 1. Она включает в себя признаки.

Первым этапом, подлежащим анализу, является формирование концепции разрабатываемой системы. Для проведения анализа необходимо использовать одну из разновидностей FMECA - Concept FMECA [12]. *Concept FMECA* анализ направлен на выявление проблем в основных функциях системы. Объектами Concept FMECA анализа являются требования к системе, функции системы, подсистемы и компоненты, описанные в техническом задании. Основной задачей CFMECA является выбор оптимальных концептуальных альтернатив или определения изменений в спецификации проектируемой системы. Все потенциальные виды отказов и эффекты каждой предлагаемой концепции рассматриваются прежде, чем приступить к реальной конструкции [6].

Таблица 1

Классификация FMEA анализа

Признаки классификации	**Типы методик**	**XMECA**
Объект анализа	Продукты	Product FMECA Concept FMECA
	Процессы	Process FMECA
Типы продуктов (компонетов):	- Аппаратное обеспечение; - Интерфейсы	Design FMECA FMVEA
	Программное обеспечение	Software FMECA, FMVEA
	Системы	System FMECA
Принципы анализа	- Сверху-вниз; - Снизу-вверх; - Анализ компонентов; - Анализ функций	Hierarchical (X)MECA
Анализируем свойства	Надежность	FMEA
	Функциональная безопасность	FMECA FMEDA FMVEA
	Информационная безопасность	Intrusion MECA FMVEA

После проведения CFMECA и устранения несоответствий следует перейти на следующий этап разработки конструкции, на котором проводится *Design FMECA* [6]. Design FMECA анализ направлен на выявление проблем в компонентах и подсистемах изделия. Объектом Design FMECA является конструкция изделия. Использование Design FMECA помогает улучшить и предотвратить разработку недостаточно отработанной конструкции устройства, тем самым предупреждая риски и дефекты устройства за счет:

– учета требований для изготовления, сборки и удобства обслуживания;

– рассмотрения всех видов потенциальных дефектов конструкции и их последствий;

– анализа информации при планировании мероприятий по испытанию конструкций;

– ранжирования всех дефектов и установки приоритетов для последующего улучшения показателей или устранения дефектов конструкции.

Впоследствии проводится разновидность анализа, которая называется *Process FMECA*. Process FMECA представляет собой процедуру анализа

первоначально разработанного и предложенного (процесса) производства и доработки этого процесса в ходе работы соответствующей PFMEA-команды (Process FMECA команды). Объектом PFMEA являются технологические процессы такие как операции, переходы и т.д. Целью PFMEA является проведение анализа на этапе разработки производственного процесса и это позволяет предотвратить внедрение в производство недостаточно отработанных процессов.

Назначение PFMECA:

– выявление потенциальных дефектов процесса изготовления данного технического объекта, приводящих к дефектам данного технического объекта;

– оценивание реакции потребителя на соответствующие дефекты;

– выявление потенциальных факторов процессов изготовления и сборки и вариации процессов, требующих усиленных действий для снижения частоты (вероятности) дефектов или для обнаружения условий дефектов процесса;

– составление ранжированного списка потенциальных дефектов процесса, устанавливая этим систему приоритетов для рассмотрения корректирующих действий;

– документирование результатов процесса изготовления или сборки.

Этап проектирования и разработки программного обеспечения для устройства анализируется с помощью *Software FMECA* [13]. Объектом анализа используя Software FMECA являются VHDL модули системы. Для проведения Software FMECA следует выполнить следующие шаги:

– разбить программное обеспечение на компоненты, модули и функции;

– описать функцию каждого компонента системы, определенного в системной структуре;

– определить корректность, отказы и неисправности роботы каждой процедуры или метода в компонентах системы,;

– расчет RPN для каждого вида отказов функций и компонентов;

– определение мер по усовершенствованию программного обеспечения путем предотвращения возможных неисправностей или ошибок или оптимизированного обнаружения сбоев.

Для разработки систем критического применения важными требованиям являются требования как к функциональной, так и к информационной безопасности. После завершения этапа их разработки следует этап тестирования. Самым ответственным моментом на этапе тестирования является анализ уязвимостей системы, поскольку каждая уязвимость посредством атак злоумышленниками может привести к сбою или отказу системы.

Для предотвращения этого следует провести анализ системы на уязвимости с помощью одной из разновидностей FMECA – Intrusion MECA. IMECA является модификацией FMECA-метода, которая учитывает возможные вторжения в систему. Объектом IMECA являются уязвимости системы. Во время оценки систем IMECA может быть использована в дополнение к стандартизированным FMECA для доменов связанных с безопасностью, потому что каждая из уязвимостей может стать отказом в случае вторжения в такие системы [6, 13-14].

Разновидностью IFMECA, которая учитывает требования к функциональной и информационное безопасности, является FMVECA, Failure Modes, Effects and Vulnerability Analysis, во время которого компоненты системы (как аппаратные, так и программные) не только анализируются на выявление режимов отказов, но и на выявление режимов угроз [15]. В качестве причины угрозы информационной безопасности, рассматриваются уязвимости [16].

Анализ V-модели жизненного цикла критических систем

Процесс разработки систем на базе FPGA требует строго формализованных процессов проектирования, верификации и валидации.

Регламентированной моделью ЖЦ разработки и обеспечения функциональной безопасности критических систем на базе FPGA является V-модель [17]. Эта модель доработана с учетом аспекта информационной безопасности из стандарта IEC 61508 в [18] (рисунок 1).

Компонентами представленной V-модели жизненного цикла являются:

– входная информация – требования и архитектура к системе;

– выходной этап – использование, включающее процедуры модификации системы;

– этапы разработки системы – разработка требований и архитектуры системы, проектирование, разработка программных модулей и кодирование;

– этапы верификации – выполнение верификации на каждом этапе разработки полученного продукта на соответствие входным требованиям, а также верификация проводится на этапах тестирования модулей;

– валидация на соответствие исходным требованиям.

Прямоугольники отражают мероприятия, которые связаны с этапами жизненного цикла, а различные типы стрелок отражают связи между ними.

В таблице 2 для каждого из этапов жизненного

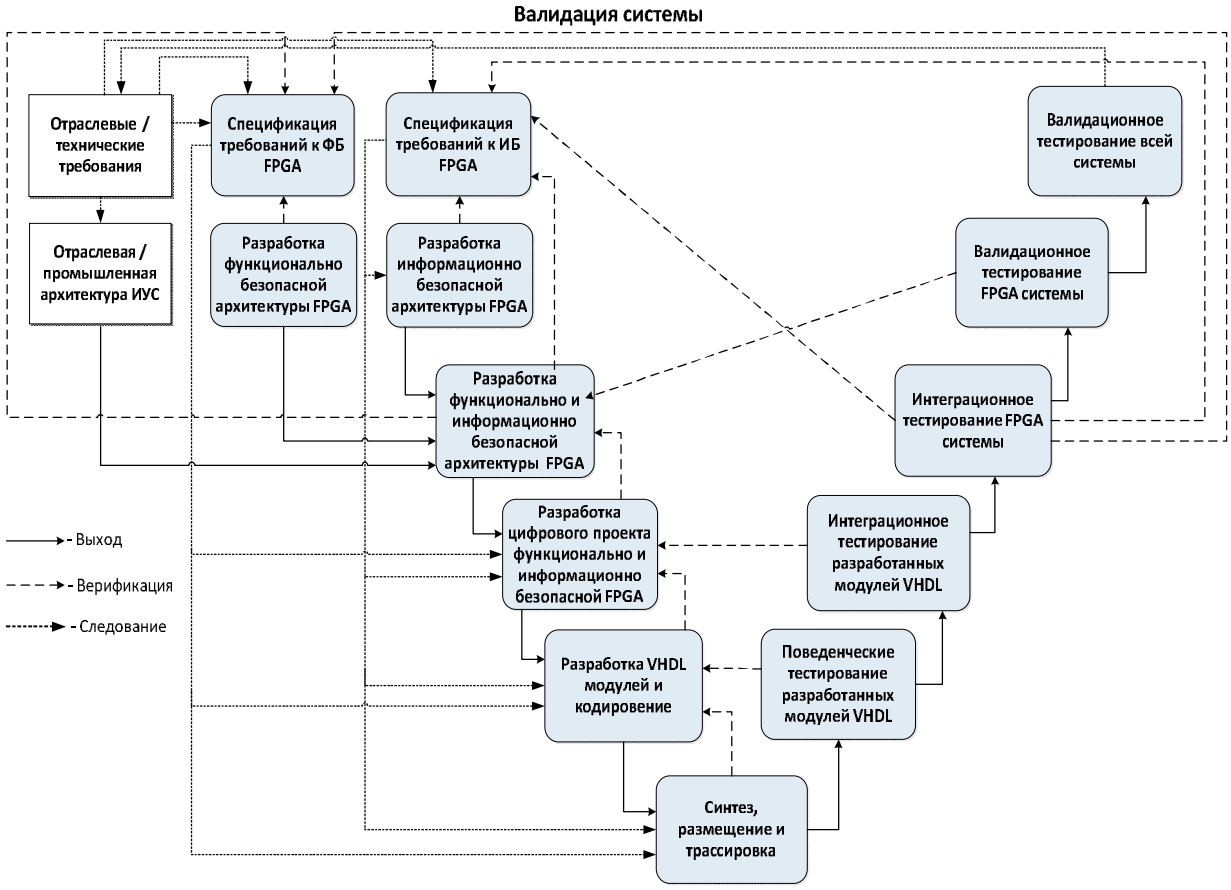

Рис. 1. V-модель жизненного цикла разработки функционально и информационно безопасных проектов на FPGA

Таблица 2

Применение XMECA на этапах ЖЦ разработки систем на базе FPGA

Этап ЖЦ	Цель этапа	Входная информация	Выходная информация	Тип XMECA
Спецификация требований к функциональной и информационной безопасности FPGA	Получение требований, включающих в себя требования к функциональной и информационной безопасности и требования архитектуре	Требования к разрабатываемой системе	Спецификация требований к системе	Concept FMECA Intrusion MECA(IMECA) FMVEA
Разработка функционально и информационно безопасной архитектуры FPGA	Разработка архитектуры системы, которая позволит реализовать все требования к функциональной и информационной безопасности и заданной архитектуре. Выбор инструментальных средств разработки, верификации и валидации	Спецификация требований к системе.	Описание архитектуры системы. План интеграционного тестирования компонентов системы. Набор необходимых инструментальных средств. Правила кодирования	Design FMECA
Разработка цифрового проекта функционально и информационно безопасной FPGA	С помощью выбранного программного обеспечения разработать цифровой проект FPGA системы, которая соответствует всем требованиям.	Описание архитектуры системы. Набор инструментальных средств	Цифровой проект на FPGA	Process FMECA
Разработка VHDL модулей и кодирование.	Представление системы в виду модулей, их описание и кодирование на языке VHDL.	Проект VHDL модулей системы. Правила кодирования. Набор инструментальных средств автоматизированного проектирования, синтеза и моделирования	Проект VHDL модулей системы. План тестирования модулей Программный код. Результаты анализа программного кода	Software FMECA
Синтез, размещение, трассировка	Синтез проекта на VHDL. Размещение проекта заданной FPGA.			

Окончание табл. 2

Этап ЖЦ	Цель этапа	Входная информация	Выходная информация	Тип XMECA
Поведенческое тестирование разработанных VHDL модулей	Верификация требований к безопасности программных модулей (каждый модуль должен выполнять только требуемые функции)	План тестирования модулей. Программный код. Результаты анализа программного кода	Отчет о поведенческом тестировании модулей. Верифицированные программные модули	Software FMECA FMVEA
Интеграционное тестирование разработанных модулей на VHDL.	Верифицирование требований к безопасности системы компонентов и модулей.	План интеграционного тестирования модулей и компонентов системы.	Отчет о интеграционном тестировании модулей и компонентов. Верифицированные модули системы.	Intrusion MECA(IMECA) FMVEA
Интеграционное тестирование FPGA системы			Верифицированная система.	
Валидационное тестирование FPGA системы.	Обеспечение соответствия интеграционного тестирования к требованиям функциональной безопасности.	Спецификация требования к системе. План валидации системы	Отчет о валидации системы. Валидированная система	System FMECA
Валидационное тестирование всей системы				

цикла разработки систем на базе FPGA представлены достигаемые цели, а также входные, выходные информационные потоки и тип рекомендуемого FMECA. Предложенный вариант использования разновидностей метода XMECA представляет собой комплекс рекомендаций для анализа систем на этапах жизненного цикла.

Заключение

В данной работе проанализированы разновидности метода XMECA и особенности их применения для систем на FPGA. Основным результатом работы является комплекс рекомендаций по применению XMECA для анализа процессно-продуктных аномалий (отказов, несоответствий и т.д.) на этапах жизненного цикла системы. Эти рекомендации адресованы различным элементам V-модели ЖЦ, модифицированной с учетом требований по функциональной и информационной безопасности.

Дальнейшие исследования могут быть направлены на более строгую формализацию и комплексирование процедур XMECA по входам-выходам и создания на этой основе модифицированной модели жизненного цикла безопасности, а также полную автоматизацию процессов оценивания.

Литература

1. Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis(FMEA) [Электронный ресурс]. – Режим доступа: https://webstore.iec.ch/preview/info_iec60812%7Bed2.0%7Den_d.pdf. – 28.03.2016.

2. Risk Analysis Method: FMEA/FMECA in the Organizations [Электронный ресурс]. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.2246&rep=rep1&type=pdf. – 30.03.2016.

3. Методи системного аналізу в радіоелектроніці та комп'ютерній інженерії [Текст] : підруч. для студентів ВНЗ / А. В. Горбенко та ін. ; за ред. С. Ю. Данчишиної, В. С. Харченка ; Ін-т інновац. технологій і змісту освіти, Нац. аерокосм. ун-т ім. М. Є. Жуковського "ХАІ". - Харків : ХАІ, 2014. – 423 с.

4. FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment [Text] / edits V. S. Kharchenko, V. V. Sklyar. – Kharkiv : National Aerospace University "KhAI", 2008. – 188 p.

5. Fault Insertion Testing of FPGA-based NPP I&C Systems: SIL Certification Issues [Text] / V. S. Kharchenko, V. V. Sklyar, O. N. Odarushchenko, A. O. Ivasyuk // Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication. ICONE22-31175. – Prague, Czech Republic., 7-11 July 2014. – 5 p.

6. Rausand, M. System Analysis. Failure Modes, Effects, and Criticality Analysis [Электронный ресурс] / M. Rausand. – Режим доступа: http://www.fmeainfocentre.com/presentations/fmeca.pdf. – 29.03.2016.

7. Illiashenko, O. Choosing FMECA-Based Techniques and Tools for Safety Analysis of Critical Systems [Text] / O. Illiashenko, E. Babeshko // Information & Security: An International Journal. – 2012. – No. 28(2). – P. 275-285.

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

9. FMEA and FMECA [Электронный ресурс]. – Режим доступа: http://www.fmeainfocentre.com/updates/jun09/FMEA%20and%20FMECA.PDF. – 30.03.2016.

10. FMEA Glossary of Terms [Электронный ресурс]. – Режим доступа: http://www.effectivefmeas.com/uploads/Glossary_of_FMEA_Terms.pdf. –30.03.2016.

11. Warwick manufacturing group. Product Excellence Using Six Sigma. Failure Modes, Effects & Criticality Analysis [Электронный ресурс]. – Режим доступа: http://www2.warwick.ac.uk/fac/sci/wmg/ftmsc/modules/modulelist/peuss/slides/section_12a_fmeca_notes.pdf. – 30.03.2016.

12. An Ontological Approach to Systematization of SW-FMEA [Text] / I. Bicchierai, G. Bucci, C.Nocentini, E. Vicario // Lecture Notes in Computer Science. – 2012 – Vol. 7612. – P. 173-184.

13. Gorbenko, A. F(I)MEA-technique of Web Services Analysis and Dependability Ensuring [Text] / A. Gorbenko, V. Kharchenko, O. Tarasyuk, A. Furmanov // Lecture Notes in Computer Science. – 2006. – Vol. 4157. – P. 153-167.

14. Babeshko, E. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring [Text] / E. Babeshko, V. Kharchenko, A. Gorbenko // Third International Conference on Dependability of Computer SystemsDEPCOS-RELCOMEX, 2008. – P. 309-315.

15. Schmitter, C. FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles [Text] / C. Schmitter, M. Zhedong, P. Smith // Computer Safety, Reliability, and Security. Lecture Notes in Computer Science. – 2014. – Vol. 8696. – P. 282-288.

16. Security Application of Failure Mode and Effect Analysis (FMEA) [Text] / C. Schmitter, T. Gruber, P. Puscher, E. Schoitsch // Computer Safety, Reliability, and Security. Lecture Notes in Computer Science. – 2014. – Vol. 8666. – P. 310-325.

17. Security Informed Safety Assessment of Industrial FPGA-Based Systems. Proceedings of Probabilistic Safety Assessment and Management PSAM 12. [Электронный ресурс] / V. Kharchenko, O. Illiashenko, V. Brezhnev, A. Boyarchuk, V. Golovanevskiy. – Режим доступа: http://psam12.org/proceedings/paper/paper_489_1.pdf. – 30.03.2016.

18. IEC 61508:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safetyrelated Systems, 2010.

References

1 *Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA)*. Available at: https://webstore.iec.ch/preview/info_iec60812%7Bed2.0%7Den_d.pdf (accessed 28.03.2016).

2. *Risk Analysis Method: FMEA/FMECA in the Organizations* Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.2246&rep=rep1&type=pdf (accessed 28.03.2016).

3. Gorbenko, A. V. Kharchenko, V. S. and others. *Metody systemnoho analizu v radioelektronitsi ta komp"yuterniy inzheneriyi* [Methods of system analysis in radio electronics and computer engineering]. Kharkiv, National Aerospace University Publ., 2014. 423 p.

4. Kharchenko, V. S., Sklyar, V. V. (Edits). *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment*. Kharkiv, National Aerospace University KhAI Publ., 2008. 188 p.

5. Kharchenko, V. S., Sklyar, V. V., Odarushchenko, O. N., Ivasyuk, A. O. Fault Insertion Testing of FPGA-based NPP I&C Systems: SIL Certification Issues. *Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication. ICONE22-31175*. Prague, Czech Republic, 2014. 5 p.

6. Rausand, M. *System Analysis. Failure Modes, Effects, and Criticality Analysis.* Available at: http://www.fmeainfocentre.com/presentations/fmeca.pdf (accessed 29.03.2016).

7. Illiashenko, O., Babeshko, E. Choosing FMECA-based techniques and tools for safety analysis of critical systems. *Information & Security: An International Journal*, 2012, no. 28(2), pp. 275-285.

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

9. *FMEA and FMECA*. Available at: http://www.fmeainfocentre.com/updates/jun09/FMEA%20and%20FMECA.PDF (accessed 29.03.2016).

10. *FMEA Glossary of Terms*. Available at: http://www.effectivefmeas.com/uploads/Glossary_of_FMEA_Terms.pdf (accessed 30.03.2016).

11. Warwick manufacturing group. Product Excellence Using Six Sigma. *Failure Modes, Effects & Criticality Analysis*. Available at: http://www2.warwick.ac.uk/fac/sci/wmg/ftmsc/modules/modulelist/peuss/slides/section_12a_fmeca_notes.pdf (accessed 01.04.2016).

12. Bicchierai, I., Bucci, G., Nocentini, C., Vicario, E. An Ontological Approach to Systematization of SW-FMEA. *Lecture Notes in Computer Science,* 2012, vol. 7612, pp. 173-184.

13. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A. F(I)MEA-technique of Web Services Analysis and Dependability Ensuring. *Lecture Notes in Computer Science*, vol. 4157, 2006, pp. 153-167.

14. Babeshko, E., Kharchenko, V., Gorbenko. A. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring. *Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX*, 2008, pp. 309-315.

15. Schmitter, C., Zhedong, M., Smith, P. FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles. *Computer Safety, Reliability, and Security. Lecture Notes in Computer Science*, vol. 8696, 2014, pp. 282-288.

16. Schmitter, C., Gruber, T., Puscher, P., Schoitsch, E. Security Application of Failure Mode and Effect Analysis (FMEA). *Computer Safety, Reliability, and Security. Lecture Notes in Computer Science*, vol. 8666, 2014, pp. 310-325.

17. Kharchenko, V., Illiashenko, O., Brezhnev V., Boyarchuk A., Golovanevskiy V., Security Informed Safety Assessment of Industrial FPGA-Based Systems. Proceedings of Probabilistic Safety Assessment and Management PSAM 12. Available at: http://psam12.org/proceedings/paper/paper_489_1.pdf (accessed 02.04.2016)

18. *IEC 61508:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safetyrelated Systems*, 2010.

Поступила в редакцию 04.04.2016, рассмотрена на редколлегии 14.04.2016

ОЦІНКА БЕЗПЕКИ СИСТЕМ НА FPGA З ВИКОРИСТАННЯМ XMECA ДЛЯ V-МОДЕЛІ ЖИТТЄВОГО ЦИКЛУ

О. О. Ілляшенко, В. С. Харченко, Я. А. Чуйков

У статті проведено аналіз переваг і недоліків методу XMECA для оцінки безпеки різних компонент і видів відмов (X) системи. Досліджено особливості застосування XMECA на основних етапах життєвого циклу системи. Проведено аналіз V-моделі життєвого циклу розробки систем на базі програмованої логіки. Запропоновано комплекс рекомендацій щодо застосування XMECA для аналізу процесно-продуктних аномалій (відмов, невідповідностей і т.д.) для V-моделі життєвого циклу розроблення систем на базі FPGA. Ці рекомендації адресовані різним елементам V-моделі, модифікованої з урахуванням вимог до функціональної та інформаційної безпеки.

Ключові слова: FMEA, життєвий цикл, ризики, відмови, функціональна безпека, інформаційна безпека.

SAFETY ANALYSIS OF FPGA-BASED SYSTEMS USING XMECA FOR V-MODEL OF LIFE CYCLE

O. A. Illiashenko, V. S. Kharchenko, Y. A. Chuikov

The article describes analysis of advantages and lacks of XMECA approach in application for safety assessment of various components and failures (X) of a particular system. The features of the application of XMECA technique at key stages of system lifecycle are reviewed. The V-model of development lifecycle of programmable logic based system was analyzed. It was proposed set of recommendations concerning using of XMECA for analysis of process and product anomalies (failures, discrepancies, etc.) for the V-model of development life cycle of FPGA based systems. These recommendations are addressed to the different elements of V-model, which is modified taking into account requirements to safety and security.

Key words: FMECA, lifecycle, risks, failures, safety, security.

Ильяшенко Олег Александрович – ассистент, младший научный сотрудник кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: o.illiashenko@csn.khai.edu.

Харченко Вячеслав Сергеевич – д-р техн. наук, профессор, зав. каф. компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: v_s_kharchenko@ukr.net.

Чуйков Ярослав Анатольевич – аспирант каф. компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: chuikov_yaroslav@mail.ru.

Illiashenko Oleg Aleksandrovych – Assistant Lecturer, Junior Research Fellow of Department of Computer Systems and Networks, National Aerospace University n. a. N. Ye. Zhukovsky “KhAI”, Kharkov, Ukraine, e-mail: o.illiashenko@csn.khai.edu.

Kharchenko Vyacheslav Sergeevich – Dr. Sc. in Engineering, Prof., Head of Department of Computer Systems and Networks, National Aerospace University n. a. N. Ye. Zhukovsky “KhAI”, Kharkov, Ukraine, e-mail: v_s_kharchenko@ukr.net.

Chuikov Yaroslav Anatol'evich – Phd student, Department of Computer Systems and Networks, National Aerospace University n. a. N. Ye. Zhukovsky “KhAI”, Kharkov, Ukraine e-mail: chuikov_yaroslav@mail.ru.