полнялось условие $r \leq d$. Подмножества выходов можно объединять в одну группу, если на данных подмножествах выходов одновременное проявление ошибок при внутренних неисправностях исключено. Для каждой контролируемой группы реализуется своя схема контроля, а затем выходы различных схем контроля объединяются на входах самопроверяемого компаратора.

3 Метод синтеза схемы контроля на основе полиномиальных кодов, обнаруживающих определенные виды ошибок. Согласно классификации ошибок в кодовых векторах могут возникать следующие виды ошибок: одиночные, монотонные, симметричные и асимметричные ошибки [4]. Одиночные ошибки связаны с искажениями только одного разряда, монотонные, симметричные и асимметричные – двух и более. Если искажаются только нулевые или только единичные разряды, то ошибка считается монотонной, иначе – симметричной или асимметричной. Симметричная ошибка имеет четную кратность и связана с одинаковым числом искажаемых нулевых и единичных значений. Асимметричная ошибка – это ошибка, связанная с неравным количеством искажений нулевых и единичных разрядов. В ходе исследования полиномиальных кодов установлено, что некоторые образующие полиномы позволяют строить коды с полным обнаружением ошибок определенных видов [5]. В таком случае, для построения схемы контроля с идентификацией полного множества ошибок анализируются все возможные виды ошибок на выходах устройства. Далее формируются группы контролепригодных по полиномиальным кодам выходов устройства. Для этого из множества выходов выделяются такие, на которых проявляются только симметричные или только асимметричные ошибки. Выходы с одноименным видом ошибок помещаются в одну группу. Для каждой сформированной группы реализуется своя контрольная схема.

В конечном счете, при проектировании систем на основе рассмотренных методов выбирается метод, позволяющий синтезировать самопроверяемое устройство с минимальной структурной избыточностью.

Приведенные выше методы синтеза схем встроенного контроля на основе полиномиальных кодов позволяют получать устройства, имеющие свойство обнаружения полного множества ошибок с наименьшими аппаратурными затратами.

Список литературы

1 Control Systems: Theory and Applications / V. Kuntsevich [et al.] // River Publishers Series in Automation, Control and Robotics, 2018.

2 Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В. В. Сапожников [и др.] ; под ред. Вл. В. Сапожникова. – М. : Транспорт, 1995. – 272 с.

3 Надежность и эффективность в технике: Справочник в десяти томах. Т. 9: Техническая диагностика / под ред. В. В. Клюева и П. П. Пархоменко. – М. : Машиностроение, 1987. – 352 с.

4 **Сапожников, В. В.** Коды с суммированием для систем технического диагностирования : [монография] / В. В. Сапожников, Вл. В. Сапожников, Д. В. Ефанов. – Т. 1: Классические коды Бергера и их модификации. – М. : Наука, 2020. – 383 с.

5 **Abdullaev, R.** Polynomial Code with Detecting the Symmetric and Asymmetric Errors in the Data Vectors / R. Abdullaev [et al.]. // Proceedings of 17th IEEE East-West Design & Test Symposium (EWDTS`2019), Batumi, Georgia, September 13–16. – 2019. – P. 157–161. – DOI: 10.1109/EWDTS.2019.8884451.

УДК 658.56

ОСОБЕННОСТИ ПРОВЕДЕНИЯ FMECA МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

И. О. ЖИГАЛИН, С. И. ХОМЕНКО, И. В. ЛОГВИНЕНКО
Белорусский государственный университет транспорта, г. Гомель

FMECA (Failure Mode, Effects and Criticality Analysis) – это инструмент для анализа потенциальных отказов, их последствий и критичности. Метод применяется при оценке соответствия требованиям по функциональной безопасности и предназначен для выявления потенциальных отказов, причин их возникновения и последствий при эксплуатации [1]. Эффективность FMECA заключается в том, что, благодаря усилиям на начальной стадии, можно добиться соответствия заданным ТНПА требованиям по функциональной безопасности на последующих этапах жизненного цикла продукта. Кроме того, исключение потенциальных отказов позволяет существенно снизить количество доработок до соответствия требованиям по функциональной безопасности.

FMECA – обязательный этап подтверждения соответствия процессорных систем требованиям безопасности микроэлектронных блоков и устройств железнодорожной автоматики и телемеханики и рассматривается как методика по снижению рисков, что актуально при производстве продукции, к которой предъявляются особые требования по безопасности (SIL4) [2]. Результаты FMECA включают в доказательство безопасности микроэлектронных блоков, устройств и систем железнодорожной автоматики и телемеханики (СЖАТ).

Этапы проведения FMECA-анализа:

– определяется объект исследования и собирается команда экспертов. Для сложной, составной структуры четко очерчиваются границы, в рамках которых проводится анализ.

– составляется список тех элементов объекта, которые могут привести к возникновению отказов.

– для выбранных на предыдущей стадии объектов анализируются потенциальные отказы, их критичность.

При анализе FMECA требуется хорошая конструкторская документация для полного понимания принципов функционирования системы в целом и ее отдельных узлов, так как при недостаточном качестве документации возможны разночтения в понимании принципов работы отдельных узлов, что в дальнейшем потребует дополнительных консультаций с разработчиками аппаратного и программного обеспечения (ПО) и усложняет процесс проведения анализа. По результатам FMECA возможна корректировка аппаратных средств.

Сложности анализа микроэлектронных СЖАТ заключаются в трассировке требований до отдельных функциональных блоков и необходимости анализа последствий отказов во всех режимах работы системы.

Для большинства блоков и устройств СЖАТ необходимо проведение моделирования процессов. При этом предпочтительно проводить проверку на стенде, имитирующем реальный узел, с имитацией отказов. Введение отказов при анализе может привести к выходу узла из строя или изменению параметров, входящих в него элементов. На данный момент существует возможность программного схемотехнического моделирования узлов электронных устройств. Но здесь возникает риск некорректного результата моделирования из-за особенностей ПО или неверных установок параметров моделирования. В сложных схемах выделяются и моделируются отдельные ответственные узлы, которые на взгляд эксперта могут приводить к опасным отказам. При этом возникают сложности с выбором параметров входных воздействий на узел, учитывающих все возможные состояния. Также при моделировании узлов сложно учесть всю возможную совокупность изменений параметров группы элементов (в допустимых пределах).

В схемах с высокой плотностью монтажа сложно анализировать короткое замыкание (КЗ) между выводами, т.к. они расположены на небольшом расстоянии и отсутствуют технические решения, позволяющие исключить КЗ (покрытие непроводящим лаком). Например, при расстоянии между выводами в 1 мм, в радиус 3 мм попадает до 28 выводов, с которыми требуется проанализировать последствия КЗ. В таких случаях можно анализировать не все близкорасположенные выводы, а выявлять сочетания выводов, КЗ между которыми могут приводить к опасных отказам. Например, КЗ выводов интерфейсов различных типов с динамическими сигналами будет выявлено соответствующими контроллерами и не приведет к опасным последствиям (защитный отказ).

При моделировании требуется применять программные модели интегральных схем (ИС), которые зачастую отсутствуют в базе ПО системы моделирования. Программные модели ИС можно получить от производителя, но в некоторых случаях разработчик модели не учитывает ряд критичных параметров, используя упрощенную функциональную модель. Введение отказа не позволяет с полной уверенностью утверждать правильность результата моделирования. При этом не все модели позволяют имитировать требуемые отказы. Кроме того, для процессорных структур существуют специфические отказы, которые в моделях не предусмотрены, что не позволяет в полной мере применять моделирование. Анализируя процессорные системы, требуется учитывать не только аппаратное обеспечение, но и ПО. Зачастую тип отказа зависит от того, как ПО среагирует на отказ.

При анализе существует возможность исключить из рассмотрения ряд узлов, отказ которых гарантированно приводит к защитному состоянию (защищенные шины данных; блоки питания, при наличии средств контроля и т. д.). Требуется экспертная оценка возможности такого исключения, т. к. неправильное исключение из анализа потенциально опасно.

В большинстве случаев производитель ИС при составлении документации, не описывает поведение изделия при некоторых воздействиях. Например, при наличии нескольких выводов питания (земли), не указывается поведение устройства при изменении схемы подключения (обрыв, короткое замыкание

одного вывода). Также часто не указываются параметры настройки портов по умолчанию (подтягивание), что усложняет анализ при обрывах. Зачастую отсутствует информация о нагрузочной способности порта, что усложняет анализ его поведения при отказах.

Сложные ИС обычно рассматриваются на уровне функциональных блоков. Рассмотрение поэлементно затруднено, а в большинстве случаев невозможно. Однако для определения последствий отказов необходим анализ внутренней структуры блока, которая зачастую недостаточно детализирована.

Применение FMECA анализа позволяет на этапе проектирование скорректировать технические требования к ПО устройства, а при экспертизе установить правильность и целостность его функционирования. На основании маскируемых отказов можно выявить цепочку накапливаемых отказов, приводящую к опасному состоянию. Анализ цепочки позволяет рассчитать вероятность наступления опасного отказа. Большинство выявленных проблем решаются на этапе проектирования аппаратных средств и ПО при тесном взаимодействии с разработчиком микроэлектронной системы.

Таким образом, рассмотренные в докладе особенности FMECA анализа микроэлектронных СЖАТ повышают роль экспертной оценки. Поэтому при высоких требованиях по функциональной безопасности (SIL4) получение достоверной оценки требует высокой квалификации эксперта, который при неопределенности исходных данных должен оценить верхнюю границу показателей безопасности (интенсивность опасных отказов) и подтвердить соответствие этих показателей требованиям нормативных документов.

Список литературы

1 **Николаева, Н. Г.** FMEA – анализ видов и последствий отказов : учеб. пособие / Н. Г. Николаева, С. М. Горюнова. – Казань : КГТУ, 2007. – 93 с.

2 **Скляр, В. В.** Обеспечение безопасности АСУТП в соответствии с современными стандартами : метод. пособие / В. В. Скляр. – М. : Инфра-Инженерия, 2018.

УДК 656.256:519.683.7

ВЕРИФИКАЦИЯ МОДЕЛЕЙ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И ПРОГРАММИРОВАНИЯ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

А. Ю. КАМЕНЕВ, А. А. ЛАПКО, Е. В. ЩЕБЛЫКИНА
Украинский государственный университет железнодорожного транспорта, г. Харьков

Н. В. КАМЕНЕВА
Харьковское отделение филиала «Проектно-изыскательный институт железнодорожного транспорта» АО «Украинская железная дорога»

Расширение объёмов и сфер внедрения микропроцессорных систем железнодорожной автоматики (ЖА) на магистральном и промышленном транспорте предопределяет развитие методов и средств автоматизированного проектирования и программирования заложенных в них программно-аппаратных устройств. Классические системы автоматизированного проектирования (САПР) и автоматизации инженерных расчётов (CAE) в своих стандартных библиотеках, как правило, не содержат необходимых символов, функций и методов, с помощью которых возможно проектирование и программирование (в том числе конфигурирование) систем управления различных производителей. В соответствии с этим необходима разработка отдельных методов и моделей выполнения этих задач, которые могут быть интегрированы с существующими САПР- и CAE-системами.

В рамках последних исследований, проведённых в частности специалистами Украинского государственного университета железнодорожного транспорта в коллаборации со внешними стейкхолдерами, были разработаны методы, модели и средства автоматизированного проектирования и программирования систем ЖА, базируемые на графоаналитическом (в том числе графо-функциональном) представлении технологических объектов ЖА.

При этом реализация новых методов и технологий проектирования и программирования требует надлежащей верификации достоверности и адекватности заложенных в них моделей с позиции обеспечения надлежащей надёжности и безопасности функционирования устройств ЖА, являющихся продуктом указанных этапов разработки. В выполненных научно-прикладных исследованиях доказано, что для вложенных графо-функциональных моделей, закладываемых в САПР- и CAE-