УДК 656.26

С. Н. ХАРЛАП, кандидат технических наук, В. Л. КАТКОВ, магистр технических наук, Белорусский государственный университет транспорта, г. Гомель

АВТОМАТИЗАЦИЯ ПРОВЕДЕНИЯ АНАЛИЗА FMECA МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

Рассмотрены особенности использования метода FMECA для доказательства безопасности микроэлектронных систем железнодорожной автоматики и телемеханики. Рассмотрены способы имитации отказов при анализе FMECA и представлено программное обеспечение для автоматизированного проведения анализа.

В настоящее время активно разрабатываются новые микроэлектронные системы и устройства железнодорожной автоматики, связанные с обеспечением безопасности движения поездов. В соответствии с действующими стандартами к таким системам предъявляют наиболее жесткие требования по функциональной безопасности и относят к четвертому (высшему) уровню полноты безопасности УПБ 4 [1, 2]. Действия разработчика по подтверждению достигнутого уровня функциональной безопасности строго регламентированы соответствующими нормативными документами.

Нормативные документы, определяющие требования функциональной безопасности. Функциональная безопасность – это достаточно формализованное свойство, поскольку системы, важные для безопасности, являются предметом государственного лицензирования во всех странах. Поэтому все виды деятельности в области разработки безопасных систем достаточно жестко регламентированы различными стандартами.

Основополагающим «вертикальным» стандартом верхнего уровня «*Umbrella standard*» для функциональной безопасности является МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (*IEC* 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems*). Стандарт дает общее понятие о функциональной безопасности, включает в себя общие требования к организации жизненного цикла электрических, электронных, программируемых электронных (Э/Э/ПЭ) систем, связанных с безопасностью, и методы, которые могут использоваться для достижения заданного уровня полноты безопасности.

На территории Евразийского экономического союза основным документом, определяющим требования в области функциональной безопасности, является технический регламент Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта». Регламент устанавливает требования к инфраструктуре железнодорожного транспорта, включая системы железнодорожной автоматики, в целях защиты жизни и здоровья человека, окружающей среды, сохранности имущества, а также предупреждения действий, вводящих в заблуждение потребителей относительно его назначения и безопасности. В свою очередь детализация требований осуществляется с помощью ряда поддерживающих стандартов (ГОСТ) [3–5].

Метод FMECA. В соответствии с требованиями технического регламента Таможенного союза ТР ТС 003/2011 разработчик обязан выполнить ряд мероприятий по подтверждению функциональной безопасности и оформить результаты этих мероприятий в виде документа «Доказательство безопасности».

Доказательство безопасности предполагает подтверждение выполнения следующей концепции обеспечения безопасности, принятой для микроэлектронных систем [6]: «Одиночные отказы аппаратных средств и ошибки в программном обеспечении не должны приводить к опасным отказам и должны обнаруживаться до того, как в системе возникнет второй отказ». Основным методом доказательства выполнения этой концепции служит анализ видов, последствий и критичности отказов (*Failure Mode, Effects and Criticality Analysis – FMECA*) [7].

Основными этапами проведения анализа являются:

1) изучение документации на систему;
2) определение видов отказов;
3) последовательная имитация отказов;
4) определение последствий и критичности отказов;
5) анализ возможности накопления отказов, влияние отказов по общей причине.

На первом этапе выполняется анализ технической документации на систему или устройство (технических требований, архитектуры, принципиальных схем, функционального описания). Особое внимание уделяется четкой формулировке критериев опасных и защитных отказов, методам и критериям обнаружения отказов, а также возможности парирования последствий отказов. Эта информация необходима для принятия решения о критичности отказов на последующих этапах анализа. На этом же этапе выполняется предварительный анализ последствий отказов функциональных блоков, позволяющий выделить компоненты системы, отказы которых не влияют на функциональную безопасность, что позволяет исключить эти компоненты из дальнейшего анализа.

После изучения архитектуры и принципиальных схем определяются виды отказов. Для элементов систем железнодорожной автоматики определен перечень видов отказов компонентов аппаратных средств [2, приложение С]. Например, для резистора определены такие отказы, как обрыв, короткое замыкание, увеличение или уменьшение сопротивления, короткое замыкание на корпус. Существует возможность исключения некоторых видов отказов из анализа в зависимости от физических свойств компонента или технологии его изготовления. Например, короткое замыкание резистора можно исключить из анализа, если на него нанесено лакокрасочное покрытие. Результатом этого этапа является перечень видов отказов, которые должны учитываться при выполнении анализа FMECA.

На следующих этапах для каждого компонента последовательно выполняется имитация всех отказов из перечня видов отказов и определяются последствия и критичность каждого одиночного отказа, а также возможность накопления отказов и влияние отказов по общей причине. Данная процедура может быть выполнена следующими способами:

– экспертной оценкой последствий отказов без выполнения имитации;

– выполнение физического макетирования отказа с помощью специальных коммутирующих устройств, позволяющих имитировать обрывы компонентов размыканием соответствующих цепей, а короткие замыкания компонентов – замыканием определенных узлов на плате;

– внесение отказов в компьютерную имитационную модель устройства.

Способы имитации отказов при анализе FMECA. Каждый из рассмотренных выше способов имеет свои ограничения. Для проведения экспертной оценки последствий отказов без выполнения имитации необходимо привлечение высококвалифицированных экспертов. В этом случае устройство должно быть достаточно простым, чтобы эксперт мог с высокой достоверностью спрогнозировать поведение схемы при отказе. При увеличении сложности схемы достоверность результатов снижается, что требует применения других методов анализа.

Следует отметить еще одно ограничение данного метода – влияние «человеческого фактора» на достоверность результатов анализа. Количество возможных отказов, последствия которых надо анализировать, даже для относительно несложных схем измеряется сотнями и тысячами различных вариантов. Работа принимает ярко выраженный рутинный характер, что повышает вероятность человеческих ошибок при принятии решения. Учитывая высокие требования по функциональной безопасности, которые надо подтвердить анализом FMECA, для исключения влияния «человеческого фактора» необходимо привлечение как минимум двух независимых экспертов, которые либо выполняют эту работу параллельно, либо один эксперт выполняет анализ, а второй его проверяет.

Выполнение физического макетирования отказа с помощью специальных коммутирующих устройств обладает высокой достоверностью полученных результатов. Однако такой способ также имеет свои ограничения. Во-первых, это высокие затраты на имитацию отказов, т. к. требуется изготовление специального макета. Во-вторых, большое количество отказов невозможно имитировать с помощью коммутирующих устройств. Например, если обрыв резистора можно имитировать разрывом соответствующей цепи, то изменение напряжения открытия диода таким способом имитировать невозможно. Кроме того, в ряде отказов происходит разрушающее влияние на другие элементы схемы, и их имитация приведет к выходу из строя всего устройства, что потребует затрат на его восстановление. Поэтому обычно данный способ применяют в том случае, когда другими методами не удается обеспечить высокую достоверность анализа последствий отказов.

Наиболее эффективным является внесение отказов в компьютерную имитационную модель устройства. Современные пакеты схемотехнического моделирования обладают достаточно высокой достоверностью результатов и возможностью внесения различных отказов. Однако большинство программных средств имеют свои ограничения, например, *PSpice* не имеет возможности моделировать программируемые элементы, *Proteus Design Suite* имеет закрытый формат библиотек элементов, что не позволяет имитировать некоторые отказы.

Все рассмотренные способы предполагают имитацию отказов в ручном режиме, это приводит к тому, что анализ занимает длительное время. Кроме того, при использовании имитационных моделей остается не решенной проблема влияния «человеческого фактора» на достоверность результатов анализа.

Таким образом, можно выделить следующие основные проблемы, с которыми сталкиваются эксперты при выполнении анализа FMECA: высокую сложность систем, длительный и рутинный характер выполнения анализа, обуславливающий высокую вероятность ошибок человека. Частично решить эти проблемы можно автоматизацией проведения анализа FMECA на базе имитационной модели устройства.

Программное обеспечение для выполнения анализа FMECA. В научно-исследовательской лаборатории «Безопасность и ЭМС технических средств» разработано программное обеспечение, которое позволяет в автоматизированном режиме получить результаты моделирования электронной схемы при отказе различных элементов.

За основу для моделирования электронных схем была взята программа-симулятор электронных схем *ngSpice* – симулятор электронных схем общего назначения, обеспечивающий моделирование в режиме смешанных сигналов и на смешанном уровне.

Первым из достоинств данного симулятора является то, что он базируется на системе схемотехнического моделирования *SPICE*, а значит, можно выделить следующие особенности:

– большое количество проверенных библиотек с моделями электронных компонентов;

– доступный формат хранения имитационных моделей, возможность редактирования и создания новых моделей;

– возможность анализа схемных решений в различных режимах (анализ переходных процессов, моделирование статического режима работа, частотный анализ, температурный анализ и т. д.).

Вторым преимуществом является то, что у данной программы открытый исходный код, и ее использование не требует покупки лицензии, также она развивается уже более 30 лет, в ней выявлены и устранены многие ошибки.

Третье преимущество – наличие подробной документации.

Четвертым достоинство является кроссплатформенность программы.

И последним, но немаловажным преимуществом является то, что помимо версии с графической оболочкой также есть версия в виде *dll* библиотеки, которую проще использовать при разработке собственного программного обеспечения.

В отличие от программ-лабораторий (*Multisim*, *Proteus*, *OrCAD* и др.) *ngSpice* представляет собой симулятор, который не имеет своего собственного графического интерфейса, а лишь выполняет имитационное моделирование электронной схемы. Это значит, что в нем невозможно начертить схему, которую необходимо моделировать. Существует два способа создания файла-схемы, который будет загружаться в *ngSpice*:

– составление схемы по синтаксическим правилам языка *SPICE* в текстовом редакторе;

– извлечение/конвертирование графического представления схемы из редактора электрических схем.

Из-за того, что первый способ не является предпочтительным при составлении сложных схем (велика вероятность совершения ошибки при соединении элементов между собой), предлагается использовать второй способ. В результате обзора различных программных решений был сделан выбор в пользу программы

LTspice. Особо стоит отметить, что данный программный продукт является бесплатным в использовании.

Программа написана на языках *C#* и *Python*. Структура разработанного ПО приведена на рисунке 1.

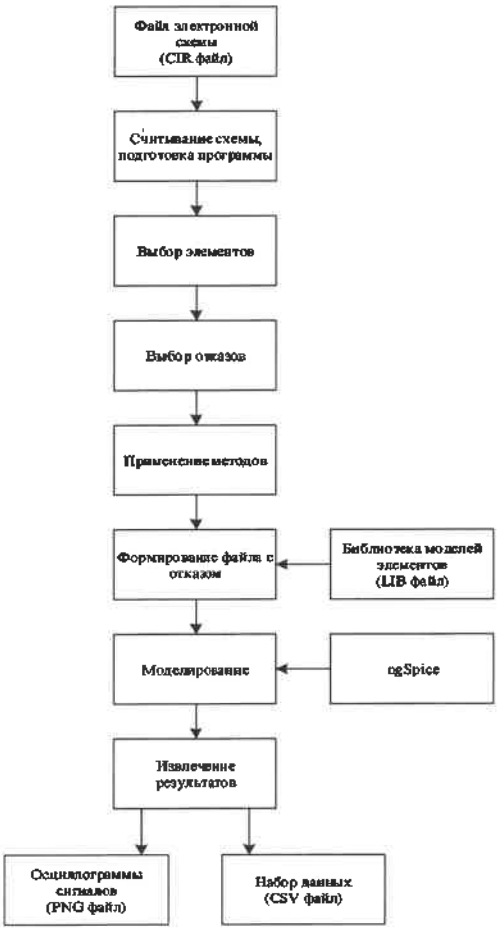

Рисунок 1 – Структура ПО

Программа имеет интуитивно понятный интерфейс (рисунок 2), с помощью которого пользователь может загрузить электронную схему и указать, какие виды отказов элементов необходимо моделировать. После запуска процесса моделирования внесение отказов и протоколирование полученных результатов происходит в автоматическом режиме.

К достоинствам разработанной программы следует отнести следующие:

– программное обеспечение базируется на программе *ngSpice* [8], которая использует для моделирования ядро *SPICE* – общепризнанный эталон в области моделирования электронных схем;

– используется открытое, свободно распространяемое программное обеспечение;

– в разработанном программном продукте есть два способа протоколирования полученных результатов: графический (осциллограммы) и текстовый (уровни напряжений во времени). Такой подход позволяет использовать как ручные методы анализа, так и средства автоматизации обработки результатов моделирования.

В научно-исследовательской лаборатории «Безопасность и ЭМС технических средств» выполнена апробация программного обеспечения при выполнении научно-исследовательских работ. Результаты автоматизированного моделирования отказов элементов в схеме совпадают с результатами, полученными при ручном внесении отказов в программе *LTspice*.

Применение разработанного программного продукта при проведении экспертизы на функциональную безопасность современных устройств ЖАТ позволит автоматизировать анализ влияния отказов каждого из элементов исследуемой схемы, повысит качество анализа электронных схем, сократит сроки выполнения работ и снизит количество ошибок, связанных с человеческим фактором.

Рисунок 2 – Главное окно программы с подготовленным заданием

Список литературы

1 **СТБ EN 50126-1–2011.** Железные дороги. Требования и подтверждение надежности, пригодности к эксплуатации, ремонтопригодности и безопасности. Часть 1. Основные требования и общий процесс. – Введ. 2011-08-01.

2 **СТБ IEC 62425–2011.** Железный дороги. Системы связи, сигнализации и обработки данных. Электронные системы сигнализации, связанные с безопасностью. – Введ. 2011-08-01.

3 **ГОСТ 33432–2015.** Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. – Введ. 2016-09-01.

4 **ГОСТ 33433–2015.** Безопасность функциональная. Управление рисками на железнодорожном транспорте. – Введ. 2016-09-01.

5 **ГОСТ 34012–2016.** Аппаратура железнодорожной автоматики и телемеханики. Общие технические требования. – Введ. 2017-10-01.

6 **Бочков, К. А.** Микропроцессорные системы автоматики на железнодорожном транспорте : учеб. пособие / К. А. Бочков, А. Н. Коврига, С. Н. Харлап. – Гомель : БелГУТ, 2013. – 254 с.

7 **ГОСТ Р 51901.12–2007.** (МЭК 60812:2006). Менеджмент риска. Метод анализа видов и последствий отказов. – Введ. 2008-09-01.

8 The open source Spice circuit simulator [Электронный ресурс] : сайт. – Режим доступа : http://ngspice. sourceforge.net/. – Дата доступа : 25.09.2020.

Получено 15.10.2020

S. N. Kharlap, V. L. Katkov. Automation of analysis of FMECA microelectronic systems of railway Signalling and Interlocking.

The features of using the FMECA method to safety case of microelectronic systems of railway Signalling and Interlocking are considered. Methods for simulating failures in FMECA analysis are considered and software for automated analysis is presented.