ний возможна только с помощью специализированных систем моделирования, разрабатываемых конкретно под поставленные задачи.

Одним из таких средств является комплекс аппаратно-программных средств для проведения имитационных испытаний на функциональную безопасность микроэлектронных и микропроцессорных систем управления ответственными технологическими процессами (КИИБ), разработанный в научно-исследовательской и испытательной лаборатории «Безопасность и ЭМС технических средств» Белорусского государственного университета транспорта. Комплекс предназначен для проведения имитационных испытаний на функциональную безопасность микропроцессорных систем управления ответственными технологическими процессами.

Комплекс позволяет выявить на стадии разработки и испытаний программно-технических средств на базе микроконтроллеров наличие аппаратных и программных компонентов, отказы и сбои которых могут нарушить функциональную безопасность системы.

Особенностью данного комплекса является имитация отказов в программной модели, полностью реализующей поведение микроконтроллера, и анализ работы неисправного микроконтроллера с загруженным в него программным обеспечением, которое будет использоваться в процессе эксплуатации.

После выполнения анализа FMEA выполняется расчет показателей безопасности, в частности интенсивности опасных отказов. Для расчета в основном применяется метод анализа дерева отказов (FTA – Fault Tree Analysis). Идея метода состоит в разложении событий, связанных с отказами (опасными отказами) системы, на элементарные события, связанные с отказами элементов или подсистем, с учётом причинно-следственных связей между событиями, полученными в результате анализа FMEA. В дальнейшем, на основе дерева отказов с помощью вероятностных методов определяются основные показатели безопасности. Полученные результаты сравниваются с предельными значениями, определяемыми нормативными документами.

Представленные выше методы и средства успешно использовались в научно-исследовательской лаборатории «БЭМС ТС» при проведении оценки устройств и систем, разработанных различными организациями.

Обзор представленных методов и средств оценки безопасности микроэлектронных схем на безопасность позволяет сделать следующие выводы:

– ввиду высокой сложности микроэлектронных схем, значительного объема выполняемых расчетов и моделирования анализ должен проводиться с привлечением различных средств автоматизации;

– из-за большого разнообразия испытуемых систем анализ выполняется по методикам, разрабатываемым для каждого типа систем индивидуально.

Поэтому использование стандартных пакетов программ для анализа на безопасность затруднено. Специфика выполнения работ по экспертизе и испытаниям требует от методов и средств автоматизации высокой гибкости, достоверности полученных результатов, автоматизации рутинных операций, документированности процесса испытаний, воспроизводимости результатов. Все эти требования можно удовлетворить только разработкой собственных специализированных программных средств, таких как КИИБ или аналогичных программных продуктов.

УДК 656.25

АВТОМАТИЗАЦИЯ ОБРАБОТКИ РЕЗУЛЬТАТОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ЭЛЕКТРОННЫХ СХЕМ В PSpice

А. Д. ЧАРУШНИКОВ
Белорусский государственный университет транспорта, г. Гомель

Устройства железнодорожной автоматики и телемеханики относятся к системам, критичным к безопасности. Одним из обязательных требований при использовании микроконтроллеров в данных системах является анализ их поведения при возникновении отказов.

Отказом называется событие, нарушающее работоспособность системы, когда хотя бы один из параметров, определяющих способность выполнять заданные функции, не соответствует требованиям документации.

Существует следующая классификация отказов:

– по влиянию на безопасность: защитные, опасные, маскируемые (могут быть обнаруживаемые и не обнаруживаемые);

– проявлению: внезапные, постепенные;

– последствиям: критические (могут создать опасность для человека), не критические.

– зависимости: зависимые, независимые, по общей причине;

– значению: константные, с непостоянным значением.

Целью имитационных испытаний на безопасность функционирования является подтверждение того, что испытываемое устройство или система при возникновении заданного класса неисправностей аппаратных и программных средств, отказах внешних датчиков и неправильных действиях человека-оператора не формирует сигналы управления, нарушающие условия безопасности движения поездов. Выполнить такой анализ другими средствами, в том числе во время лабораторных и эксплуатационных испытаний, не представляется возможным из-за значительных материальных и временны́х затрат на имитацию отказов и их устранение.

Общее количество неисправностей велико и составляет сотни отказов. Такое количество отказов приводит к значительным временны́м затратам при моделировании различных схем. Поэтому целесообразно разработать программный продукт, который автоматически будет проводить имитационные испытания на функциональную безопасность микроэлектронных схем.

Имитационные испытания проходят в несколько этапов. Составляется план испытаний, включающий всё множество проверяемых технологических алгоритмов. Для каждого технологического алгоритма определяются исходные технологические ситуации (состояния всех элементов системы и внешних датчиков) и последовательность внешних воздействий (действий операторов и изменений состояний датчиков), позволяющая однозначно проверить правильность выполнения данного алгоритма. Последовательно моделируются технологические ситуации и внешние воздействия.

Первым действием программного обеспечения является считывание файлов конфигурации. Это необходимо для анализа схемы, элементов, используемых в схеме, и их библиотек.

После считывания файлов конфигурации в соответствующем окне программы появляется список всех элементов, используемых в схеме. Из этого списка выбираем элементы, в которых необходимо имитировать отказ.

Следующим шагом является выбор отказов для выбранных элементов. Весь список отказов для этих элементов хранится в базе данных.

В базе данных существует четыре метода отказов: последовательное подключение резистора (имитация обрыва), параллельное подключение резистора (имитация короткого замыкания), параллельно-последовательное, изменение параметров модели. Для четвертого метода отказов (изменение параметров модели) необходимо знать путь к библиотеке элементов, т. е. к файлу *.LIB. В файле *.LIB содержатся все параметры интересующего нас элемента.

Когда все действия выполнились, ПО предусматривает подключение к PSpice через COM-сервер. После моделирования отказа в PSpice результат копируется и сохраняется в файле *.CSD.

Каждый отказ моделируется по определенному заранее методу. Метод моделирования отображается при выборе отказа в графе «Метод моделирования отказа».

Если методом моделирования отказа является «Последовательное включение резистора», то данные отказа заполняются в таблице «Последовательное включение элемента», в которой указаны узел элемента и подключаемый к этому узлу резистор с определенным значением.

Если отказу соответствует метод «Параллельное включение резистора», то данные об отказе заполняются в таблице «Параллельное включение элемента», в которой указываются два узла элемента, к которым подключается резистор с определенным значением.

В методе «Последовательное и параллельное включение резисторов» заполняются обе таблицы по такому же принципу.

Четвертым методом моделирования отказа является «Изменение параметров модели». Если отказ моделируется по этому методу, то данные об отказе находятся в таблице «Параметры модели». В этой таблице указаны параметры элемента и их значение, которые необходимо изменить.

Далее пользователю нужно задать интервал времени, на котором будет производиться поиск отказов по заданным критериям. В выпадающем списке уже имеется ряд интервалов, которые были созданы для данной схемы, но при желании пользователь может создать новый или изменить существующий. Далее задание критериев будет производиться для заданного интервала.

Если пользователь выбрал нужный интервал, он может приступить к заданию критериев отказов на данном интервале. Не имеет значения, критерии какого типа отказов задаются в начале, но очень важно, чтобы пользователь соблюдал последовательность задания критериев отказов для каждого отдельного интервала.

Далее пользователю необходимо выбрать первый сигнал из выпадающего списка, после чего ему станет доступен список условий, которые он может задать для данного сигнала.

Программа в автоматическом режиме сканирует все каталоги с отказами и находит в них файлы с расширением *.csd. После нахождения файла программа начинает парсить, в результате чего создается объект класса Node с парами значений «Время – Значение сигнала в этот момент времени». После этого программа пробегает по всем временным отсчетам в первом из указанных в программе интервалов и сравнивает значения сигнала в данный момент времени со значением переменной, если при задании условия была задана переменная, или со значением второго сигнала в этот же моменте времени, если при задании критериев был сигнал в качестве второй переменной. В случае, когда после анализа интервала не было выполнено условие для обнаружения отказа, то берется следующий критерий и анализируется таким же образом. В случае обнаружения отказа проверка данного интервала для заданного интервала останавливается и происходит проверка следующего критерия для данного интервала, если таковой имеется. Если больше не имеется критериев, связанных с заданным по фактору «И», то делается заключение о том, что на заданном интервале обнаружен заданный отказ.

После проверки всех критериев на заданном интервале программа переходит к анализу следующего интервала. Анализ всех последующих интервалов происходит по такому же принципу.

Анализ отказов происходит в определенной последовательности: первыми проверяются критерии опасного отказа, затем защитного отказа и в конце – необнаруживаемого отказа. Таким образом, в случае, если был обнаружен опасный отказ, то проверка в остальных отказах уже не нужна, поскольку система уже не прошла испытания на безопасность на заданном интервале.

После проверки всех критериев на всех интервалах программа создает протокол испытаний, заполняемый всей информацией, для генерации которой не нужно участие пользователя.

УДК 656.2.08

ОСОБЕННОСТИ ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПОЕЗДОВ

К. Э. ЧЕРКАСОВ
Белорусский государственный университет транспорта, г. Гомель

Одной из наиболее важных проблем железнодорожного транспорта является обеспечение безопасности. Из-за нарушений системы безопасности создается угроза или ущерб жизни и здоровью людей, наносится вред окружающей среде, утрачиваются грузы и другие значительные материальные ценности. Статистика транспортных происшествий показывает, что наиболее частой их причиной являются действия человека. Для снижения влияния человеческого фактора можно использовать систему поддержки принятия решений.

Система поддержки принятия решений – это автоматизированная компьютерная система, которая путем сбора и анализа большого количества информации может влиять на процесс принятия решений человеком, и даёт различные рекомендации в сложных ситуациях. Данная технология широко применяется в разных сферах деятельности, таких как машиностроение, транспорт, авиация, военная промышленность, бизнес, медицина, энергетика и многие другие. Использование системы поддержки принятия решений при организации движения поездов позволило бы значительно снизить риск принятия неправильного решения оперативным персоналом в критических ситуациях.

Стандартная система поддержки принятия решений состоит из четырех ключевых компонентов:

1) базы данных, которая содержит информацию об объекте;

2) базы знаний, которая содержит знания специалистов в соответствующей предметной области;