обнаружения отказов для константных отказов всех бит регистра и отказов короткого замыкания для всех смежных бит регистра, что согласуется с требованиями стандартов EN 50129 и IEC 61508.

Также рассматривается выбор пары адресов A_1 и A_2, по которым помещаются ключевые команды, реализующие переменный сигнал на внешнее устройство. Далее предлагается два варианта интеграции с существующим программным обеспечением, в контексте которых рассматривается применение метода на определённой архитектуре и особенности того или иного выбора.

Второй пример рассматривает обнаружение отказов адресной шины. По своим свойствам микропроцессорная шина отличается от регистра: у неё нет ячеек для хранения информации, но при этом доступны операции чтения и записи. Функционально шина соединяет элементы микропроцессора и служит для передачи данных между ними, и это взаимодействие можно использовать для обнаружения отказов шины. В то же время отказы адресной шины проявляют себя подобно отказам адресных ячеек памяти: если происходит константный отказ нуля младшего бита шины, то это приводит к постоянному чтению нуля с соответствующей цифровой линии. Поэтому из-за отказа будет происходить обращение к другой ячейке памяти.

Проверка адресной шины происходит в два этапа: инициализации и времени выполнения. На первом из них необходимо удостовериться, что адресная шина находится в рабочем состоянии и все адреса правильно отображаются. Например, это можно сделать по рассматриваемому методу согласно следующему алгоритму:

1) запись константы 0 во все ячейки заданного адресного диапазона;

2) для каждого адреса (т. е., N раз), один раз выполнить чтение значения по адресу и, если прочитан не 0, то адресная шина имеет отказ. Иначе записать единицу по рассматриваемому адресу;

3) если предыдущие действия не выявили отказов адресной шины, то она исправна.

Далее на втором этапе выбирается два адреса A_1 и A_2 по аналогичным принципам, как и в примере программного счётчика. Перед запуском основного цикла программы по этим адресам записывается некоторое значение K. В последующем во время основной работы программы данное значение сверяется при чтении по адресам A_1 и A_2. В докладе дополнительно рассматриваются адаптации описанного метода для более приемлемых для разработчиков решений, так как не всегда программа может позволить не использовать число K, а также не всегда возможно разделить адресное пространство на три части с границами по адресам A_1 и A_2.

На втором примере показывается, что метод обнаружения отказов на основе доступности адресных данных может использоваться для адресной шины микропроцессора, что метод адаптируем к прикладным потребностям разработчиков и верификаторов, может интегрироваться с другими методами и подходами, и также что он не зависит от микропроцессорной архитектуры.

Таким образом, в докладе рассматриваются характерные микропроцессорные адресные элементы: программный счётчик и адресная шина, отличающиеся от регистров общего назначения микропроцессоров. На их примере показано, что метод обнаружения отказов на основе доступности адресных данных может быть использован для множества устройств адресации совместно с другими методами обнаружения отказов.

Адресные элементы повсеместно входят в состав микропроцессорных систем и для СОБД подлежат обязательной верификации и проверке в реальном времени. Описанный метод и его примеры показывают, что он позволяет решать различные ключевые задачи обеспечения отказоустойчивости и безопасности микропроцессорных систем железнодорожной автоматики и телемеханики.

УДК 656.25

МЕТОДЫ И СРЕДСТВА ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

С. Н. ХАРЛАП

Белорусский государственный университет транспорта, г. Гомель

В настоящее время системы управления движением поездов активно оснащаются сложными технологическими комплексами и оборудованием с широким использованием информационных технологий. Важнейшей характеристикой таких систем является функциональная безопасность,

т. е. способность надежно и корректно выполнять заданные функции, обеспечивающие безопасное функционирование объектов контроля и управления.

В соответствии с действующими нормативными документами разработчик выполняет комплекс мероприятий по подтверждению количественных и качественных показателей безопасности функционирования в соответствии с заявленным уровнем обеспечения безопасности (по IEC 61508). Результатом выполнения этих мероприятий является документ «Доказательство безопасности», который подлежит обязательной экспертизе в аккредитованной лаборатории.

При анализе качественных и количественных требований безопасности проверяется их обоснованность и корректность декомпозиции структуры технических средств ЖАТ на подсистемы с учетом их влияния на безопасность. Затем выполняется анализ схемных решений и анализ видов и последствий отказов (FMEA – Failure Modes and Effects Analysis). Целью анализа является проверка того, что устройство при возникновении заданного класса отказов аппаратных средств не формируют сигналы управления и сигнализации, нарушающие условия безопасности движения поездов. Для сложных систем анализ проводится в виде моделирования.

Такой подход регламентирован международными (IEC 61508), европейскими (EN 50126, EN 50129), российскими и белорусскими нормативными документами. В данных нормативных документах определен следующий алгоритм анализа соответствия системы требованиям функциональной безопасности.

На первом этапе определяется перечень учитываемых неисправностей элементов, который формируется на основе соответствующих нормативных документов. Каждая неисправность из перечня последовательно вносится в схему, и выполняется анализ поведения системы по следующим критериям:

– нарушение условий безопасности классифицируется как опасный отказ;

– регистрация неисправности и блокировка системы классифицируется как защитный отказ;

– остальные случаи классифицируются как маскируемый отказ, допускающий накопление неисправностей и требующий дальнейшего анализа.

Выполняется расчет вероятности возникновения кратных неисправностей и, в случае, если эта вероятность больше допустимой, имитируются кратные неисправности (на практике двукратные неисправности имитируются всегда, трехкратные – только в случае накопления отказов или при возникновении зависимых отказов). Система соответствует требованиям функциональной безопасности, если в результате анализа не обнаружено ни одного опасного отказа, а вероятность возникновения кратных отказов, приводящих к опасным последствиям, не превышает нормативного значения.

Как видно из алгоритма, при проведении анализа необходимо вносить различные отказы в структуру устройства. Имитация отказов на реальном устройстве (например, перемычками) затруднительна, так как этот способ очень затратен ввиду разрушающего характера испытаний. Поэтому одним из основных способов анализа является компьютерное моделирование. Моделирование функционирования аппаратных средств без программируемых элементов выполняется в среде моделирования PSpice.

В стандартном пакете PSpice внесение отказов в схему производится вручную. Большое количество элементов и большое число видов неисправностей для каждого элемента приводит к тому, что анализ занимает длительное время. Значительная часть работы имеет рутинный характер, что приводит к повышению вероятности человеческой ошибки.

В настоящее время в ИЛ БЭМС ТС разработаны средства автоматизации проведения испытаний в пакете PSpice. Данное ПО позволяет загрузить PSpice-модель исследуемой схемы и получить перечень элементов. Затем пользователь может выбрать элементы, отказы которых будут моделироваться, а также выбрать перечень моделируемых отказов для каждого типа элементов. Программное обеспечение поддерживает функции администрирования базы данных отказов. В базе данных хранятся сведения о видах отказах применительно к каждому элементу электронной схемы, а также способ имитации каждого отказа. После запуска на моделирование программное обеспечение вносит отказы в PSpice-модель схемы и запускает COM-сервер PSpice. Результаты моделирования сохраняются в отдельной папке на диске. Разработанное ПО позволяет значительно сократить сроки проведения имитационных испытаний и повысить их достоверность.

Однако PSpice не позволяет вносить неисправности в программируемые элементы, такие как микроконтроллеры, микросхемы памяти, программируемые таймеры, порты ввода-вывода. Существующие средства отладки также не позволяют это выполнить. Поэтому реализация этих требова-

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.