этом году пущены в опытную эксплуатацию системы компьютерной и процессорно-релейной централизации стрелок и сигналов. Разрабатываются и проходят испытания другие микроэлектронные устройства. При внедрении таких устройств и систем должна быть решена задача подтверждения соответствия показателей безопасности функционирования установленным нормам, то есть должно быть выполнено доказательство безопасности.

Одним из основных элементов доказательства безопасности является подтверждение того, что система при возникновении заданного класса неисправностей аппаратных средств не формирует сигналы управления и сигнализации, нарушающие условия безопасности движения поездов. Единственным рекомендуемым методом анализа является метод полного перебора. Перечень учитываемых неисправностей определяется соответствующими нормативными документами, например, стандартом EN50129 или Памяткой ОСЖД Р-801/1.

Большинство неисправностей, таких как обрывы выводов и короткие замыкания, можно имитировать введением данных неисправностей непосредственно в испытываемый образец. Однако данный способ имитации имеет существенные недостатки, такие как трудоемкость внесения неисправностей и восстановления работоспособности устройства, а также разрушающий характер некоторых неисправностей, что значительно увеличивает сроки и стоимость проведения испытаний. Поэтому основным способом анализа является имитационное моделирование в среде PSpice. Имитация обрывов и коротких замыканий в этом случае выполняется введением в модель электрической схемы дополнительных перемычек и резисторов.

Однако в перечень учитываемых неисправностей включены неисправности элементов, которые данным способом имитировать невозможно. Это такие неисправности, как увеличение и уменьшение напряжения открытия выпрямительного диода, увеличение остаточного тока между парными электродами биполярного транзистора и др. Для имитации отказов такого типа необходимо изменение параметров PSpice-моделей полупроводниковых элементов.

В научно-исследовательской и испытательной лаборатории «Безопасность и ЭМС технических средств» выполнены исследования возможности имитации неисправностей изменением значений параметров PSpice-моделей полупроводниковых элементов. Было установлено, что некоторые отказы имитировать таким образом затруднительно. Например, обрывы коллектора и базы биполярного транзистора можно имитировать увеличением объемного сопротивления соответствующей области (RB или RC) до величины порядка 10^{10}–10^{12} Ом. В то же время аналогичное увеличение сопротивления области эмиттера RE не дает результатов. Поэтому в данном случае моделирование должно производиться включением последовательно с эмиттером резистора с сопротивлением 10^{10}–10^{12} Ом. Таким образом, для решения задачи имитации всего перечня неисправностей необходимо использовать комплексный подход, включающий как корректировку соответствующих значений параметров PSpice-моделей, так и внесение изменений в схему соединений.

Разработаны методы имитации неисправностей согласно перечням, приведенным в EN50129 и Р-801/1, которые были опробованы при анализе микроэлектронных схем блоков управления переездными светодиодными светофорами. В настоящее время разрабатываются средства автоматизации проведения анализа на безопасность функционирования.

УДК 656.259.1:004

ИСПЫТАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ ПРОЦЕССОРНО-РЕЛЕЙНОЙ ЦЕНТРАЛИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

С. Н. ХАРЛАП, О. А. ШМЫГОВСКАЯ
Белорусский государственный университет транспорта

Важнейшей характеристикой систем управления движением поездов является способность надежно и достоверно выполнять функции, обеспечивающие безопасность движения поездов (функциональная безопасность). Проблемы, связанные с функциональной безопасностью, стали сейчас

крайне актуальными в связи с широким внедрением нового поколения систем железнодорожной автоматики и телемеханики, в которых функции обеспечения безопасности реализованы программным способом.

В процессорно-релейной централизации стрелок и сигналов (ПРЦ), разработанной БелГУТом и КТЦ Белорусской железной дороги, основные функции по обеспечению безопасности, в том числе замыкание маршрутов, выполняет программное обеспечение ядра системы. Поэтому в соответствии со стандартом ОСТ 32.146-2000 при лабораторных испытаниях ПРЦ в НИЛ «Безопасность и ЭМС технических средств» отдельно проводились испытания программного обеспечения ПРЦ.

Причинами нарушения безопасного функционирования программных средств могут быть как дефекты собственно программного обеспечения (ошибки проектирования, алгоритмизации, программирования), так и внешние воздействия (сбои и отказы аппаратуры, искажения в каналах связи, ошибки персонала при эксплуатации). Поэтому целью испытаний программного обеспечения ПРЦ на соответствие требованиям функциональной безопасности являлось подтверждение не только корректности собственно программного обеспечения, но и безопасного поведения программного обеспечения при воздействии внешних дестабилизирующих факторов. Решить данную задачу с помощью одного вида испытаний (например, тестирования ПО) невозможно.

Поэтому испытания на функциональную безопасность программного обеспечения системы ПРЦ представляют собой комплекс мероприятий по подтверждению показателей безопасности функционирования, включающий техническую экспертизу программной документации; тестирование и аналитическое доказательство корректности; имитационные испытания; лабораторные испытания; испытания в условиях эксплуатации.

Основным методом обнаружения ошибок в программном обеспечении является их тестирование. В качестве наиболее важных тестов принимаются типовые технологические ситуации, характерные для области использования разрабатываемой системы. В этом случае проверка функциональной корректности обычно предусматривает полный перебор всех типовых ситуаций с учетом ошибочных действий операторов и отказов внешних датчиков. Такое тестирование называется испытаниями технологических алгоритмов на функциональную безопасность.

К сожалению, даже для относительно несложных программ тестирование не может доказать отсутствие в них ошибок, а может только обнаружить некоторую их часть. Поэтому тестирование должно в обязательном порядке дополняться аналитическим доказательством корректности наиболее критичных с точки зрения безопасности модулей программного обеспечения.

Анализ функционирования программных средств при возникновении неисправностей аппаратных средств выполнялся в рамках имитационных испытаний. Имитационные испытания являются в настоящее время самым сложным и наукоемким видом испытаний программного обеспечения. Для их проведения в испытательной лаборатории «Безопасность и ЭМС технических средств» разработан «Комплекс для проведения имитационных испытаний микропроцессорных систем железнодорожной автоматики на функциональную безопасность» (КИИБ).

Комплекс аппаратно-программных средств КИИБ предназначен для проведения ускоренных имитационных испытаний на функциональную безопасность в соответствии с IEC 61508, EN 50126, ОСТ 32.146 микропроцессорных систем управления ответственными технологическими процессами, в том числе систем управления движением поездов.

С помощью комплекса КИИБ можно имитировать отказы и сбои аппаратуры, искажение входной информации, генерацию тестов и протоколирование результатов испытаний.

Имитационные испытания обязательно дополняются лабораторными испытаниями. Лабораторные испытания включают в себя комплексное тестирование системы и испытания на функциональную безопасность при воздействии электромагнитных помех.

Испытания в условиях эксплуатации совмещаются с опытной эксплуатацией системы. Основной проблемой этих испытаний является разработка и обеспечение процедуры внесения изменений в программное обеспечение, которая должна предусматривать анализ последствий корректировки программного обеспечения и, при необходимости, его повторные испытания.

Все рассмотренные виды испытаний программных средств направлены на обнаружение различных дестабилизирующих факторов, нарушающих условия безопасного функционирования системы. Они взаимно дополняют друг друга, и только комплексное применение всех рассмотренных методов проведения испытаний позволяет добиться высокой надежности и функциональной безопасности микропроцессорных и компьютерных систем железнодорожной автоматики и телемеханики.