

По универсальности, доступности и эффективности технология реализации взаимодействия приложений баз данных в распределенных системах на основе XSQL servlet превосходит все ранее используемые подходы для решения подобных проблем.

УДК 656.256

ОЦЕНКА СРЕДСТВ ДОКАЗАТЕЛЬСТВА ПРАВИЛЬНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ПОМОЩЬЮ ТЕСТИРОВАНИЯ

Б. В. СИВКО

Белорусский государственный университет транспорта

К программному обеспечению (ПО) устройств железнодорожной автоматики и телемеханики (ЖАТ) предъявляются повышенные требования по обеспечению уровня надёжности и безопасности его функционирования. Особенно это актуально при внедрении новых устройств ЖАТ на микроэлектронной базе. При разработке и применении таких устройств необходимы эффективные методы и средства устранения ошибок ПО.

Активными методами поиска ошибок являются тестирование, доказательство правильности и метод экспертной оценки. Данные методы используются для поиска и устранения ошибок ПО, но их применение в отдельности не гарантирует нахождения всех ошибок. В устройствах систем ЖАТ наличие даже нескольких потенциальных ошибок является недопустимым. Поэтому для таких систем необходимо использовать все доступные методы поиска ошибок.

При создании методов и средств проведения доказательства правильности необходимо оценивать, насколько эффективно проводится доказательство: какие классы ошибок они способны обнаружить, насколько дорого обходится доказательство с точки зрения ресурсов и времени, насколько эффективно доказательство на разных этапах проведения, насколько глубоко нужно проводить формализацию системы при использовании ПО в сложных аппаратно-программных комплексах. Одним из методов оценки является сравнение результатов проведения доказательства правильности с результатами поиска ошибок с помощью других методов, в том числе и с методом тестирования.

В больших программах тестирование неспособно обнаружить все ошибки, а полное тестирование возможно только для малых модулей. В связи с этим для оценки методов и средств доказательства правильности возможно проведение полного тестирования малых модулей с последующим сравнением с результатами проведения верификации. В этом случае в процессе тестирования происходит обнаружение всех ошибок в ПО и возможна оценка эффективности проведения доказательства правильности.

В настоящее время в научно-исследовательской лаборатории «Безопасность и ЭМС технических средств» Белорусского государственного университета транспорта проводится апробация методов доказательства корректности ПО для ряда устройств ЖАТ. Для оценки используемых методов и средств проводится сравнение результатов с другими методами поиска ошибок на различных малых тестируемых модулях.

В докладе рассматриваются особенности оценки методов и средств доказательства правильности и перспективы данного способа улучшения качества ПО.

УДК 656.2.08:621.315

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ НЕИСПРАВНОСТЕЙ ЭЛЕКТРОННЫХ СХЕМ ПРИ АНАЛИЗЕ ИХ НА БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ

С. Н. ХАРЛАП, А. А. КОРОЛЕВ

Белорусский государственный университет транспорта

В настоящее время идет процесс внедрения на Белорусской железной дороге современных микроэлектронных и компьютерных систем железнодорожной автоматики и телемеханики. Только в

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 пере-ездными 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