УДК 656.25

МЕСТО ИМИТАЦИОННЫХ ИСПЫТАНИЙ В ДОКАЗАТЕЛЬСТВЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

С. Н. ХАРЛАП, О. А. КУЗНЕЦОВА

Белорусский государственный университет транспорта

Обязательным этапом разработки современных микроэлектронных систем железнодорожной автоматики является создание документа «Доказательство безопасности». Основным способом анализа безопасности функционирования, определенным в нормативных документах Российской Федерации и Республики Беларусь, являются имитационные испытания.

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 временных затрат на имитацию отказов и их устранение.

Однако несмотря на это, в настоящее время имитационные испытания используются в основном как вспомогательное средство при проведении экспертизы схемных решений и программного обеспечения. Это обусловлено несколькими причинами.

Во-первых, главным требованием при проведении имитационных испытаний является адекватность моделей. На рынке программных продуктов присутствует много различных средств схемотехнического моделирования, таких как *PSpice, Micro-Cap, APLAC, DesignLab, Electronics Workbench, CircuitMaker, OrCAD* и др., которые обладают достаточно большим разбросом результатов моделирования. Хотя *PSpice* в настоящее время является лидером в области моделирования микроэлектронных схем, рекомендации по его использованию для имитационных испытаний систем железнодорожной автоматики в нормативной документации отсутствуют. Положение усложняется тем, что модели некоторых современных микросхем отсутствуют, а использование аналогов приводит к дополнительным погрешностям.

Во-вторых, существующие средства схемотехнического моделирования могут быть использованы лишь частично из-за отсутствия возможности моделирования неисправностей элементов либо их неполноты. Например, *CircuitMaker* позволяет моделировать короткие замыкания и обрывы выводов элементов, но более сложные отказы, такие как изменение параметров, функциональные отказы интегральных микросхем, нужно моделировать вручную, с помощью дополнительных элементов (ключей, резисторов и т.д.) или непосредственно изменяя параметры элементов схемы. Моделирование таким образом неисправностей значительно замедляет выполнение испытаний и вносит дополнительные погрешности.

В-третьих, ни одна система моделирования не позволяет имитировать работу сложных аналого-во-цифровых схем с использованием программируемой логики и микроконтроллеров. Существующие эмуляторы, поставляемые фирмами-разработчиками микроконтроллеров, непригодны для целей анализа безопасности функционирования, так как не поддерживают имитацию отказов микроконтроллеров и работу в реальном масштабе времени. Разработка же собственных средств моделирования связана со значительными временными затратами и последующим доказательством адекватности моделей.

В-четвертых, в нормативных документах не определены методики проведения имитационных испытаний, требования к системам моделирования, перечень моделируемых отказов и их кратность.

Имитационные испытания являются самыми трудоемкими испытаниями, для проведения которых необходимы высококвалифицированные специалисты в области схемотехники и программирования. В то же время доказать безопасность функционирования сложных микроэлектронных и компьютерных систем без имитационных испытаний невозможно.

Можно выделить несколько видов имитационных испытаний, отличающихся целью и используемыми моделями. Испытания технологических алгоритмов проводятся на исправных технических средствах или моделях с целью подтверждения безопасного функционирования при отказах внешних датчиков и неправильных действиях оператора. Для имитации внешних датчиков и действий оператора разрабатывается имитатор технологических ситуаций. Испытания аппаратных средств при сбоях и отказах выполняются с использованием пакета схемотехнического моделирования *PSpice* с целью доказательства отсутствия отказов и сбоев элементов, приводящих к опасному отказу всей системы. Имитационные испытания программно-технических средств выполняются с помощью разработанного в лаборатории «Безопасность и ЭМС технических средств» программного комплекса для проведения имитационных испытаний на безопасность функционирования КИИБ. При этом моделируются различные неисправности программируемых БИС и определяются достоверность контроля исправности вычислительных каналов и способность обнаружения отказов средствами программного обеспечения.

Проведение имитационных испытаний требует значительных подготовительных работ, включающих в себя анализ функционирования изделия, определение временных и электрических характеристик на входах и выходах отдельных частей схемы, разработка недостающих моделей и их аттестация, определение критериев опасного отказа для каждой части схемы и разработка программ и методик имитационных испытаний на безопасность функционирования.

Для более широкого применения имитационных испытаний необходимо включить имитационные испытания на безопасность функционирования в перечень обязательных испытаний при сертификации систем железнодорожной автоматики, разработать или дополнить существующие нормативные документы по испытаниям на безопасность функционирования конкретными методиками, регламентирующими вопросы выбора системы моделирования, виды и кратность моделируемых отказов и способы их имитации. В этом случае имитационные испытания, проводимые в разных испытательных лабораториях и разработчиками систем, будут иметь одинаковые результаты и станет возможным их взаимное признание.

УДК 656.25-52

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ СОСТОЯНИЕМ УСТРОЙСТВ АВТОМАТИКИ

В. И. ШАМАНОВ, А. В. ПУЛЬТЯКОВ
Иркутский государственный университет путей сообщения

Внедрение микропроцессорных систем телеконтроля, телеизмерения и удаленного мониторинга позволяет ставить задачи оптимизации процессов эксплуатации больших технических систем, к которым относятся и системы железнодорожной автоматики и телемеханики (ЖАТ). Такой задачей является минимизация расходов ЖАТ при использовании более передового метода технического обслуживания – "по состоянию".

Поведение больших технических систем удобно описывать с использованием математического аппарата цепей Маркова, однако надежность системы при проявлении деградационных процессов лучше описывается так называемыми "стареющими законами", учитывающими далекую предысторию. Марковскую аппроксимацию процессов старения можно обеспечить за счет нелинейного преобразования – квантования по уровню случайных функций, характеризующих изменение во времени обобщенного параметра устройства или системы.

Такое нелинейное преобразование вполне естественно для систем ЖАТ, так как при их эксплуатации параметры измеряются обычно в дискретные и, как правило, равноотстоящие моменты времени. Математическая модель такого процесса включает в себя вектор-столбец, задающий вероятностное распределение состояний в нулевой момент времени, и стохастическую матрицу вероятностей переходов из одного состояния в другое.

Для практического применения наиболее удобны эргодические матрицы, у которых из каждого состояния можно попасть в любое другое состояние и предельные значения вероятностей состояний не зависят от начальных условий. Матрица-строка предельных вероятностей для эргодических цепей может быть найдена согласно теореме Маркова возведением матрицы переходов в достаточ-