АВТОМАТИКА, ТЕЛЕМЕХАНИКА И СВЯЗЬ

УДК 656.25

К. А. БОЧКОВ, доктор технических наук; С. Н. ХАРЛАП, кандидат технических наук; Белорусский государственный университет транспорта, г. Гомель; В. Н. ШУБАДЕРОВ, главный инженер; Белорусская железная дорога, г. Минск

ТРЕБОВАНИЯ К МЕТОДАМ ПРОВЕДЕНИЯ ИСПЫТАНИЙ НА БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

Обоснована необходимость создания единых требований к методам проведения испытаний на функциональную безопасность микроэлектронных систем железнодорожной автоматики. Раскрыта роль имитационных испытаний в процессе доказательства безопасности функционирования. Сформулированы принципы проведения испытаний на безопасность.

Создание микропроцессорных и компьютерных систем железнодорожной автоматики и телемеханики (СЖАТ) неразрывно связано с совершенствованием и развитием методов обеспечения требуемого уровня их безопасности и надежности. Основным методом проверки работоспособности и оценки надежности и безопасности таких систем являются испытания на безопасность функционирования.

Общей целью испытаний является обеспечение заданного уровня безопасности и надежности. Испытания должны проводиться на всех этапах создания систем. При этом неограниченное увеличение числа контрольно-испытательных работ не обеспечивает роста надежности и безопасности СЖАТ. Вследствие этого вся совокупность испытаний требует оптимизации, определения оптимального сочетания видов испытаний, их объема, количества и места в ходе технологических процессов проектирования и разработки СЖАТ, исходя из необходимости обеспечения требуемой безопасности, надежности, стоимости и длительности цикла изготовления и других факторов. Появление в последние годы ряда международных стандартов, посвященных обеспечению безопасности функционирования микроэлектронных систем управления ответственными технологическими процессами [1], в том числе обеспечению функциональной безопасности систем железнодорожной автоматики [2–4], отражает необходимость в доработке действующих в Республике Беларусь нормативных документов и приведение их в соответствие с международными нормами.

Следует отметить, что в настоящее время нет единой общепринятой системы испытаний микроэлектронных СЖАТ, а существует большое разнообразие методов испытаний, зависящих от особенностей и назначения испытываемой СЖАТ (или группы СЖАТ), условий производства, имеющихся традиций, уровня отработанности технологических процессов и т. д. Более того, пока нет даже единой терминологии для отдельных этапов и видов испытаний. Это приводит к необходимости отработки самих систем контроля и испытаний в каждом конкретном случае, проверки их эффективности и достоверности, т. е. к выполнению различного рода оценок надежности, калибровок, сравнения с элементарными испытаниями, а также других работ, часто включаемых в методику проведения испытаний [5, 6]. Результатом этого являются удорожание испытаний, различная степень надежности и достоверности испытаний, увеличение длительности испытаний и т. д.

Наиболее ярко эти проблемы проявляются при проведении имитационных испытаний, которые являются основным способом анализа безопасности функционирования сложных микропроцессорных устройств и систем.

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 основ-

ном 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 [6], рекомендации по его использованию для имитационных испытаний систем железнодорожной автоматики в нормативной документации отсутствуют.

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 из перечисленных систем моделирования не позволяет имитировать работу сложных аналогово-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, для их проведения 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. Методика испытаний заключается в последовательном введении отказов (коротких замыканий, обрывов, трансформаций полупроводниковых элементов и др.) в соответствии с «Каталогом возможных повреждений и отказов элементов устройств СЦБ» [7].

Имитационные испытания программно-технических средств выполняются с помощью специализированных программных комплексов, позволяющих исследовать программируемые БИС с выполняющейся управляющей программой при возникновении в них отказов и сбоев. В испытательной лаборатории «Безопасность и ЭМС технических средств» Белорусского государственного университета транспорта такие испытания выполняются с помощью программного комплекса для проведения имитационных испытаний на безопасность функционирования (КИИБ).

КИИБ позволяет выполнить имитационные испытания микропроцессорных систем на базе различных типов процессоров. Имеется опыт испытаний систем с использованием микроконтроллеров *Microchip*, *Atmel*, цифровых сигнальных процессоров *ADSP* и др., в том числе многопроцессорных систем.

Программный комплекс расширяем, адаптация под новые типы процессоров выполняется разработкой или корректировкой соответствующих моделей и их интеграцией в существующее программное обеспечение.

При проведении испытаний моделируются различные неисправности программируемых БИС и определяются достоверность контроля исправности вычислительных каналов и способность обнаружения отказов средствами программного обеспечения. Испытания проходят в автоматическом режиме без участия человека-оператора, что имеет существенное значение, учитывая объем и длительность (для сложных систем более сотни часов моделирования) испытаний. Данный комплекс являлся участником выставки-ярмарки «ЭКСПОЖД-2001», где был награжден медалью «Лауреат ВВЦ».

Имитационные испытания требуют проведения значительных подготовительных работ, включающих в себя анализ функционирования изделия, определение временных и электрических характеристик на входах и выходах отдельных частей схемы, разработку недостающих моделей и их аттестацию, определение критериев опасного отказа для каждой части схемы и разработку 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.

Программа испытаний СЖАТ должна строиться согласно определенным принципам, учитывающим специфику их конструкции, условия эксплуатации, условия производства, стоимость и т. д. Сформулируем основные из них:

1 Испытания должны обеспечивать достоверную информацию и создание системы с требуемым уровнем безопасности.

2 Испытания должны быть построены таким образом, чтобы имеющиеся дефекты выявились на более ранних этапах изготовления, на более низких уровнях разработки, т.е. операции контроля и испытаний целесообразно проводить по времени как можно ближе к тем этапам разработки и изготовления, при которых возможно возникновение ожидаемых дефектов. Это возможно только при параллельной организации хода разработки системы и ее испытаний и широком использовании имитационных испытаний.

3 Программа должна содержать испытания на все виды технологических ситуаций, которые могут возникнуть в процессе эксплуатации системы.

4 Испытания должны проводиться при воздействии внешних факторов, виды которых определяются нормативными документами. Ряд воздействующих факторов может создаваться имитацией. Испытания могут проводиться при воздействии как одного, так и комбинации нескольких факторов. Последовательность приложения внешних воздействий при испытаниях должна соответствовать последовательности их приложения при реальном функционировании системы.

5 Уровень испытательных нагрузок (электромагнитных помех, температур, вибраций и др.) должен обеспечивать необходимый запас по данному типу воздействия. Отказы при неоправданно жестких, завышенных условиях испытаний могут привести к ненужным переделкам конструкции, ее усложнению, к необходимости повторных более широких испытаний и в конечном счете к неоправданной потере времени и средств.

6 При испытаниях на безопасность функционирования необходимо учитывать комплексное воздействие различных факторов эксплуатации, таких как электромагнитные помехи различного вида, колебания температуры и влажности.

7 Испытания на комплексное воздействие факторов эксплуатации должны проводиться на возможно более высоком уровне разработки, желательно на полностью собранном и отлаженном макетном образце. К этому времени в результате предыдущих испытаний дефектные элементы уже выявлены и заменены годными и при испытаниях на комплексное воздействие выявляются дефекты, возникающие в результате взаимного влияния отдельных элементов друг на друга. Такие испытания должны обязательно включаться в программу приемочных испытаний.

8 Испытания на безопасность функционирования должны обязательно учитывать влияние сбоев аппаратных средств под воздействием различного вида электромагнитных помех (испытания на ЭМС).

9 Результаты предыдущих испытаний должны использоваться или учитываться при проведении испытаний на более высоком уровне, т. е. не должно быть дублирования.

10 Испытания на правильность и безопасность функционирования необходимо проводить по принципу последовательно нарастающих повторных испытаний. Это позволяет наиболее быстро выявить дефектные элементы (или группы элементов) и сократить цикл и стоимость испытаний, а также уменьшить число переделок системы и количество отказов и дефектов при более сложных испытаниях системы в целом.

11 При выявлении дефектов все они должны анализироваться, устраняться (исправлением дефекта или заменой элемента), а объект испытаний должен пройти после этого повторные испытания в установленном объеме. Повторные испытания по полной программе проводятся также при внесении принципиальных изменений в конструкцию, технологию или оборудование.

12 Испытания в необходимых случаях должны дополняться расчетами, что часто, не снижая безопасности системы, приводит к значительному сокращению объема испытаний. Однако наиболее критичные или сомнительные случаи должны быть проверены испытаниями натурных образцов.

13 Основными критериями эффективности контроля и испытаний являются безопасность, надежность системы, стоимость и длительность цикла испытаний, которые и должны учитываться в первую очередь при составлении программы испытаний и ее оптимизации.

14 Все лабораторные испытания должны быть закончены, а результаты обработаны и обобщены до проведения эксплуатационных испытаний.

15 Для достижения высокой эффективности контроля и испытаний необходимо обеспечить подробную и детальную разработку методики всех испытаний, тщательную по установленной форме регистрацию результатов, своевременный анализ и обобщение результатов испытаний, подготовку всех испытателей на высоком уровне и строгое соблюдение регламента и методики испытаний.

Предложенные принципы проведения испытаний могут стать основой унифицированной (базовой) системы испытаний на безопасность функционирования микроэлектронных систем железнодорожной автоматики. Такая система испытаний должна быть гармонизирована с действующими международными стандартами, базироваться на единых требованиях и методах испытаний и подкреплена соответствующими национальными стандартами. Системы испытаний конкретных СЖАТ должны строиться на основе подобной базовой с сохранением общей методологии, принципов, технологии испытаний, методики обработки результатов и т. д. и отличаться лишь включением или исключением каких-то конкретных видов испытаний и контроля или режимами проведения отдельных испытаний, вытекающих из специфики данной СЖАТ.

Внедрение такой системы, во-первых, даст испытательным лабораториям четкий инструмент для проведения испытаний на безопасность функционирования (как, например, стандарты по испытаниям на ЭМС, электробезопасность, стойкость к воздействию климатических факторов и т.д.). Во-вторых, такая система станет руководством для разработчиков современных систем железнодорожной автоматики и телемеханики, позволит реализовать принцип «сквозной» сертификации, нашедший широкое применение в мировой практике и рекомендуемый в соответствующих стандартах [1–4]. В этом случае сертификация проводится с начала проектирования на всех этапах создания опытной системы и включает значительные объемы моделирования и лабораторных испытаний. Реализация данного принципа способствует значительному сокращению сроков доработки и эксплуатационных испытаний, повышению надежности и функциональной безопасности системы.

Список литературы

1 IEC Standard 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems.

2 EN 50126 Draft European Standard: Railway applications – The Specification and Demonstration of Dependability, Reliability, Maintainability and Safety (RAMS).

3 EN 50128 Draft European Standard: Railway applications – Software for railway control and protection systems.

4 EN 50129 Draft European Standard: Railway applications – Hardware for railway control and protection systems.

5 Сертификация и доказательство безопасности систем железнодорожной автоматики / *В.В. Сапожников, Вл.В. Сапожников, В.И. Талалаев и др.*; Под ред. *Вл. В. Сапожникова*. – М.: Транспорт, 1997. – 28 с.

6 *Гавзов Д.В., Наседкин О.А., Белишкина Т.А. и др*. Методы и средства для проведения работ по сертификации систем и устройств железнодорожной автоматики и телемеханики.//Ж.-д. транспорт. Сер. «Сигнализация и связь» / ЭИ/ЦНИИТЭИ МПС. – 1999. – Вып.1–2.

7 Р 801/1 Памятка ОСЖД «Каталог возможных повреждений и отказов элементов устройств СЦБ».

Получено 01.07 2004

A. K. Bochkov, S. N. Khaplap, V. N. Shubaderov. The Requirements to Test Methods for Functional Safety of Railway Traffic Safety Monitoring and Control Systems.

The article proves the needs to develop the uniform requirements to tests methods for functional safety of railway traffic safety monitoring and control systems. It shows the role of simulated tests during the proof of functional safety. It formulated the main principles of tests for functional safety.