УДК 656.256: 681.32

БОЧКОВ К. А. – д.т.н., профессор (БелГУТ)
ХАРЛАП С. Н. – к.т.н., доцент (БелГУТ)
ШЕВЧЕНКО Д. Н. – к.т.н., доцент (БелГУТ)

МЕТОДЫ И СРЕДСТВА ДОКАЗАТЕЛЬСТВА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

Введение

В настоящее время системы управления движением поездов активно оснащаются сложными технологическими комплексами и оборудованием с широким использованием информационных технологий. Важнейшей характеристикой таких систем является способность надежно и достоверно выполнять заданные функции, обеспечивающие безопасное функционирование объектов контроля и управления (функциональная безопасность). Проблемы, связанные с функциональной безопасностью современных микроэлектронных систем железнодорожной автоматики и телемеханики, стали сейчас крайне актуальными.

Доказательство функциональной безопасности представляет собой комплекс мероприятий по подтверждению количественных и качественных показателей безопасности функционирования в соответствии с заявленным разработчиком системы железнодорожной автоматики уровнем обеспечения безопасности (по IEC 61508) (рис. 1)

Экспертизу проводят с целью оценки выполнения функциональных требований технического задания (ТЗ), технических условий (ТУ), эксплуатационно-технических требований (ЭТТ), количественных и качественных требований по безопасности изделий и составляющих их элементов.

Экспертиза включает:

– оценку концепции обеспечения безопасности, принятой разработчиками изделия;

– оценку принятых количественных и качественных норм и требований безопасности, их значений и методов расчета;

– проверку правильности (безошибочности) алгоритмов функционирования;

– анализ корректности и полноты критериев опасных отказов системы;

– анализ программно-аппаратных решений на соответствие утвержденным правилам и методам построения безопасных схем с учетом возможных отказов;

– анализ на полноту и корректность методик и программ испытаний на безопасность;

– анализ документов доказательства безопасности;

– оценку программного обеспечения в соответствии с ISO/IEC 9126, ISO/IEC 12207, ГОСТ 28195-89.

Наиболее сложными и затратными из них являются расчет количественных показателей безотказности и безопасности и анализ на безопасность программно-аппаратных решений с учетом возможных отказов.

Оценка принятых количественных и качественных норм и требований безопасности, их значений и методов расчета

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. Расчеты показателей надежности и безопасности проводят по утвержденным методикам.

Методы анализа надежности СЖАТ в значительной степени стандартизованы [1-6] и среди них можно выделить следующие:

– логико-вероятностный метод, метод анализа простейших потоков отказов, метод структурной схемы надежности, метод анализа дерева отказов (для анализа невосстанавливаемых подсистем);

– марковский и полумарковский метод (для восстанавливаемых подсистем);

– имитационное моделирование (для анализа последствий неисправностей при анализе безопасности функционирования систем)..

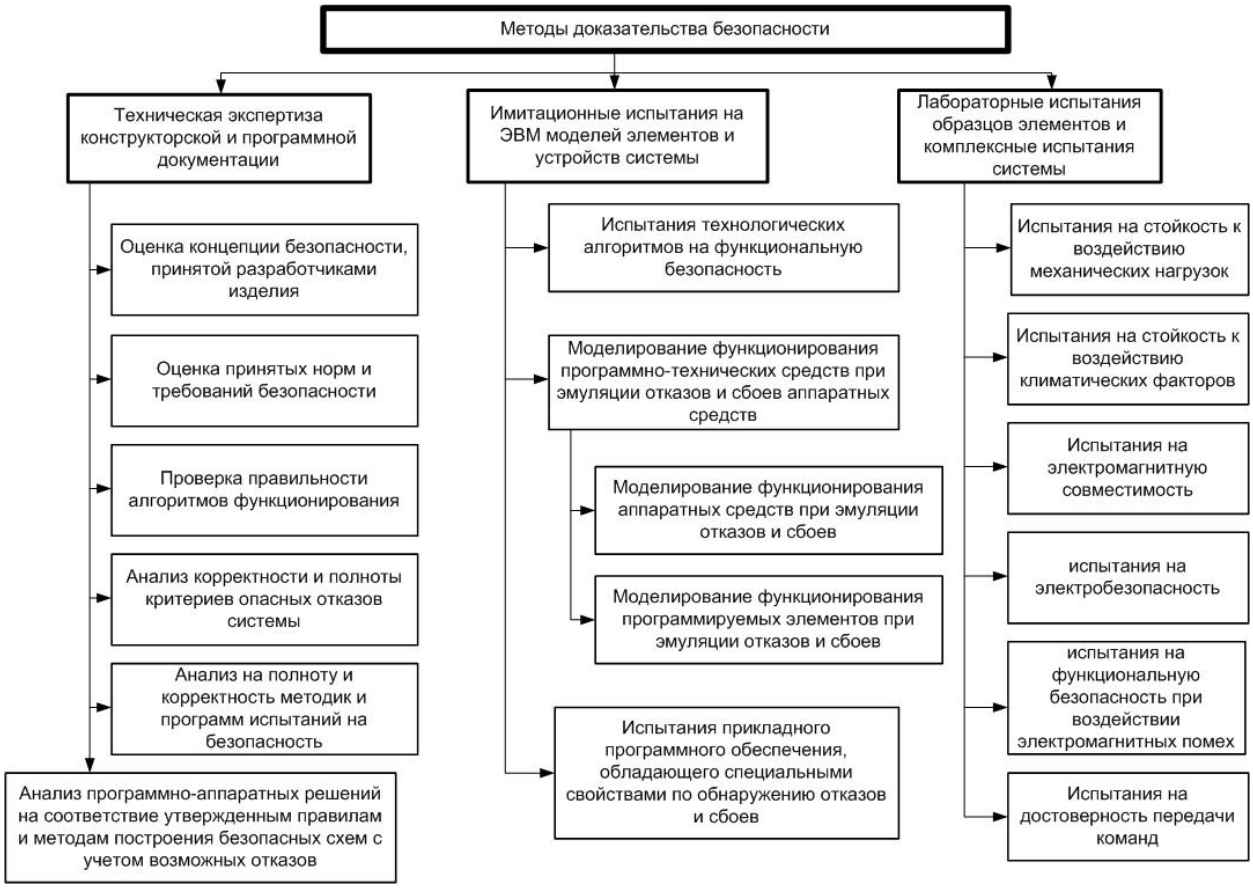

Рис. 1. Методы доказательства безопасности

– структуры технических средств ЖАТ на подсистемы с учетом их влияния на безопасность. Расчеты показателей надежности и безопасности проводят по утвержденным методикам.

Методы анализа надежности СЖАТ в значительной степени стандартизованы [1-6] и среди них можно выделить следующие:

– логико-вероятностный метод, метод анализа простейших потоков отказов, метод структурной схемы надежности, метод анализа дерева отказов (для анализа невосстанавливаемых подсистем);

– марковский и полумарковский метод (для восстанавливаемых подсистем);

– имитационное моделирование (для анализа последствий неисправностей при анализе безопасности функционирования систем).

В настоящее время существует большое количество аналитических и имитационных методов расчета надежности и безопасности функционирования систем [7-8]. Однако, применение сложных моделей надежности, адекватно отражающих свойства современных систем обеспечения безопасности (СОБ, например, систем железнодорожной автоматики, телемеханики и других систем управления ответственными технологическими процессами), ограничивается:

– большой размерностью систем;

– сложностью связей между компонентами;

– невыполнением допущений и ограничений методов, связанных с потоками отказов и восстановления системы;

– отсутствием достоверной информации о характеристиках компонентов СОБ.

Поэтому для расчета надежности и безопасности функционирования современных СОБ на этапах их разработки, сертификации, внедрения и эксплуатации попрежнему актуально применение таких методов, как логико-вероятностный метод, метод анализа дерева отказов, метод статистического моделирования. Вместе с тем, большая размерность и сложность современных систем требуют автоматизации расчетов надежности и безопасности функционирования систем.

В научно-исследовательской и испытательной лаборатории «Безопасность и ЭМС технических средств» (НИЛ БЭМС ТС) Белорусского государственного университета транспорта разработаны программные инструменты автоматизации анализа надежности следующими методами.

Логико-вероятностный метод

Одним из простейших методов анализа надежности СОБ является логико-вероятностный метод (ЛВМ), при котором структура надежности системы описывается средствами математической логики, а количественная оценка ее надежности выполняется теоретико-вероятностными методами. Наряду с вероятностью безотказной (безопасной) работы ЛВМ позволяет определять вес, значимость и вклад компонентов, что важно при разработке и сертификации СОБ [8].

Логико-вероятностный метод реализован в виде программе «Symbol Logical Calculations». Наиболее сложным этапом ЛВМ является построение математической модели надежности методом минимальных путей и сечений, что возможно лишь для структурного уровня представления СОБ. Поэтому метод применим лишь на начальных этапах разработки и сертификации СОБ. Другие ограничения ЛВМ касаются применения компонентов с тремя состояниями и не учетом последовательности отказов компонентов, что актуально при исследовании безопасности функционирования СОБ.

Метод анализа дерава отказов

Другим эффективным методов расчёта надёжности и безопасности функционирования невосстанавливаемых СКП является метод анализа дерава 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 [8]. В дальнейшем, на основе дерева отказов с помощью вероятностных методов определяются основные показатели надёжности СОБ.

Статистическое моделирование надежности

Одним из способов исследования, адекватно отражающим надёжностные свойства СОБ, является статистическое моделирование, для которого характерно получение большого числа реализаций системы или её имитационной модели на отказ с последующим статистическим анализом полученной выборки [1]. Очевидно, что для статистического моделирования надёжности СОБ на основе их имитационных моделей (ИМ) необходимо использование инструментальных средств автоматизации построения ИМ, проведения имитационных экспериментов и анализа результатов. Для этого предлагается использовать специализированный программно-технологический комплекс (ПТК) «СМ-ДЭС». Разработана технология использования ПТК для исследования надёжности и безопасности функционирования СОБ.

Кроме того, в НИЛ БЭМС ТС существуют средства автоматизации и методики качественного анализа безопасности функционирования СЖАТ на основе имитационной модели системы:

– для устройств СЖАТ на жесткой логике – «СМ-ДЭС»;

– на программируемой логике– «КИИБ».

Анализ программно-аппаратных решений на соответствие утвержденным правилам и методам построения безопасных схем с учетом возможных отказов

Анализ программно-аппаратных решений на соответствие утвержденным правилам и методам построения безопасных схем с учетом возможных отказов в виду их высокой сложности выполняется посредством имитационных испытаний.

Выделяют следующие виды имитационных испытаний:

– испытания технологических алгоритмов на функциональную безопасность;

– моделирование функционирования программно-технических средств при эмуляции отказов и сбоев аппаратных средств;

– испытания прикладного программного обеспечения, обладающего специальными свойствами по обнаружению отказов и сбоев [9].

Испытания технологических алгоритмов на функциональную безопасность

Целью испытаний технологических алгоритмов на безопасность является проверка того, что программное обеспечение испытываемого устройства при функционировании во всех режимах, предусмотренных эксплуатационной документацией, в различных технологических ситуациях, при различных действиях операторов (в том числе неправильных) и отказах внешних датчиков не формирует сигналы управления, нарушающие условия безопасности движения поездов. Испытания включают в себя:

– функциональные испытания для проверки полноты и корректности исполнения технологических алгоритмов при типовых условиях эксплуатации;

– испытания при недопустимых входных наборах данных (неправильных действиях операторов и отказах датчиков).

Перед началом испытаний составляется план испытаний, включающий все множество проверяемых технологических алгоритмов.

Для каждого технологического алгоритма определяются исходные технологические ситуации (состояния всех элементов системы и внешних датчиков) и последовательность внешних воздействий (действий операторов и изменений состояний датчиков), позволяющая однозначно проверить правильность выполнения данного алгоритма.

Для проведения испытаний (рис.2) разрабатывается имитатор технологических ситуаций позволяющий генерировать сигналы напольного оборудования. Если предполагается наличие в контуре управления человека, то разрабатывается также имитатор действий оператора.

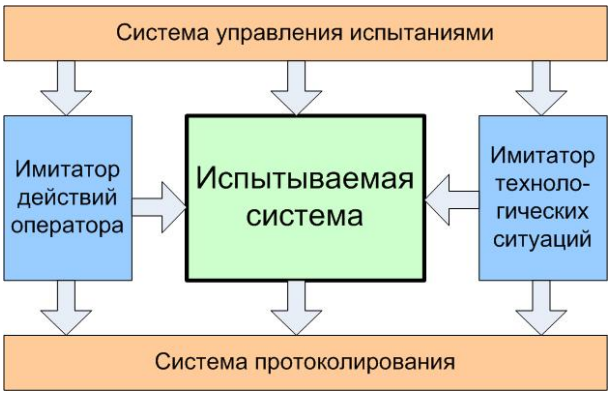

Рис. 2. Схема проведения испытаний технологических алгоритмов

Последовательно моделируются технологические ситуации и внешние воздействия. Выходные воздействия, формируемые системой, протоколируются. В некоторых случаях моделирование может производиться на реальной системе. В этом случае имитаторы технологических ситуаций не разрабатываются.

Полученные выходные воздействия сравниваются с эталонными значениями, отражающими безопасное функционирование системы.

Моделирование функционирования программно-технических средств при эмуляции отказов и сбоев аппаратных средств

Целью испытаний является проверка того, что испытываемое устройство при возникновении заданного класса неисправно-

стей аппаратных средств не формируют сигналы управления и сигнализации, нарушающие условия безопасности движения поездов. Испытания включают в себя:

– моделирование функционирования аппаратных средств (программируемые элементы отсутствуют) при эмуляции отказов и сбоев;

– моделирование функционирования программируемых элементов при эмуляции отказов и сбоев.

Оба вида испытаний имеют общую методику и различаются только использованием различных инструментальных средств моделирования.

Моделирование функционирования аппаратных средств без программируемых элементов выполняется в среде моделирования PSpice. Такой подход регламентирован международными (IEC 61508), европейскими (EN 50126, EN 50129), российскими (ОСТ 32.146, ОСТ 32.41) и белорусскими (РД РБ БЧ 19.055, РД РБ БЧ 19.057) нормативными документами.

В данных нормативных документах определен следующий алгоритм анализа соответствия системы требованиям функциональной безопасности.

Определяется перечень учитываемых неисправностей элементов, который формируется на основе соответствующих 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 считается выдержавшей испытания, если не обнаружено ни одного опасного отказа.

Как видно из алгоритма, при проведении анализа необходимо вносить различные неисправности в структуру устройства. Имитация неисправностей на реальном устройстве (например, перемычками) затруднительна, так как этот способ очень затратен в виду разрушающего характера испытаний. Поэтому одним из основных способов анализа является компьютерное моделирование в пакетах PSpice.

Выбор PSpice обусловлен следующими причинами:

– высокой достоверностью расчетов;

– PSpice является де-факто стандартом в области моделирования электронных схем;

– использованием PSpice для решения таких задач в аналогичных испытательных лабораториях других государств (например, ИЦ ЖАТ ПГУ ПС, г. С.-Петербург, Россия, ZL7, VÚŽ, Прага, Чешская Республика).

Внесение отказов в схему производится вручную. Это приводит к появлению ряда сложностей и проблем. Большое количество элементов и значительное 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 [11].

Разработанное 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 ка-

ждому 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 требований возможна только с помощью специализированных систем моделирования, разрабатываемых конкретно под поставленные задачи.

Одним из таких средств является программный комплекс КИИБ, разработанный в НИЛ «БЭМС ТС» [12].

Комплекс аппаратно-программных средств для проведения имитационных испытаний на функциональную безопасность микроэлектронных и микропроцессорных систем управления ответственными технологическими процессами (КИИБ) разработан в научно-исследовательской и испытательной лаборатории «Безопасность и ЭМС технических средств» Научно-исследовательского института железнодорожного транспорта Белорусского государственного университета транспорта.

Комплекс предназначен для проведения имитационных испытаний на функциональную безопасность в соответствии с IEC 61508, EN 50126, ОСТ 32.146 микропроцессорных систем управления ответственными технологическими процессами.

Комплекс позволяет выявить на стадии разработки и испытаний программно-технических средств на базе микроконтроллеров и компьютеров наличие аппаратных и программных компонентов, отказы и сбои которых могут нарушить функциональную безопасность системы.

КИИБ позволяет контролировать следующие характеристики:

– наличие одиночных и кратных неисправностей технических средств, приводящих к нарушению функциональной безопасности системы. Виды отказов соответствуют EN50129 и приведены на рис. 3;

– наличие ошибок программных средств, приводящих к нарушению функциональной безопасности системы;

– устойчивость функционирования при воздействии электромагнитных помех и искажениях входных сигналов;

– уровень обнаруживаемости отказов и сбоев заданной кратности средствами контроля и диагностики,

– возможность накопления отказов заданной кратности во внутренней структуре;

– тип искажения вычислительного процесса при наличии отказов технических средств.

Предусмотрены средства автоматизации испытаний, встроенный язык моделирования программы эксперимента, гибкая система настройки параметров комплекса.

Испытания прикладного программного обеспечения, обладающего специальными свойствами по обнаружению отказов и сбоев

Целью испытаний является проверка того, что прикладное программное обеспечение при возникновении заданного класса неисправностей аппаратных средств не формирует сигналы управления и сигнализации, нарушающие условия безопасности движения поездов, и генерирует контрольные сигналы, позволяющие обнаружить данные неисправности.

В качестве примеров такого программного обеспечения может служить диверситетное ПО различных каналов многоканальных систем, самопроверяемое и самотестируемое ПО и т.п.

Для проведения испытаний используют программный комплекс КИИБ.

Методика испытаний рассмотренной в предыдущем разделе. На первом этапе составляется перечень вносимых неисправностей.

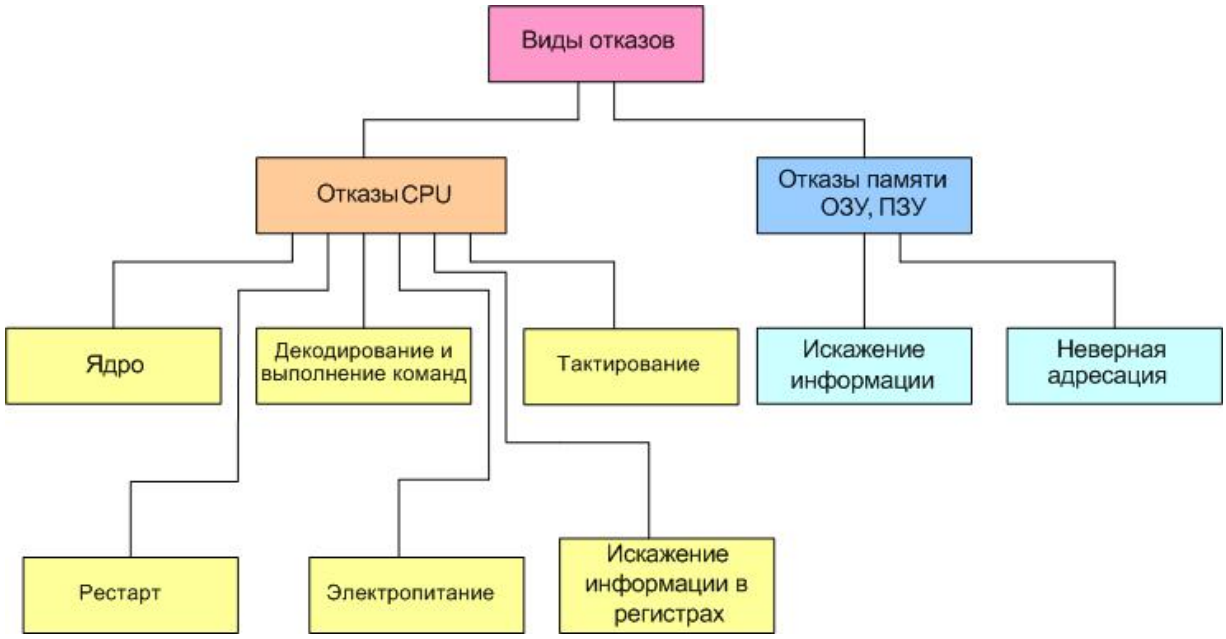

Рис. 3. Виды отказов программируемых БИС

Затем последовательно в модель вносятся одиночные неисправности из данного перечня. Выходные и контрольные сигналы, формируемые программным обеспечением, во всех допустимых режимах протоколируются и сравниваются с эталонными значениями. Делается вывод об отсутствии опасных управляющих воздействиях и о возможности обнаружения данного класса неисправностей.

Лабораторные испытания на безопасность при воздействии электромагнитных помех

Исследования, проведенные в НИЛ «БЭМС ТС» показывают, что испытания на безопасность функционирования и ЭМС необходимо проводить в комплексе, а не раздельно, как предусмотрено в действующих стандартах.

Зафиксированы случаи, когда воздействие помехами нормативного уровня (предписанного стандартами) не приводило к формированию команд управления из-за отказов аппаратуры. В то же время, воздействие электромагнитных помех с уровнями значительно ниже нормативного значения вызывало формирование сигналов управления, влияющих на безопасность движения поездов[13]. На рис. 4 представлена зависимость сбоев манипулятора «мышь» компьютеров промышленного исполнения РАС-106, от амплитуды напряжения при различных частотах**.**

Наблюдаются ярко выраженные пики, на которые приходится максимальное количество зафиксированных сбоев.

Из рис. 4 видно, что сбои происходят в достаточно узком диапазоне напряжений помех. Поэтому очень вероятна ситуация, когда при проведении испытаний на ЭМС испытатель может «не попасть» в этот диапазон и сделать заключение о соответствии системы заявленным требованиям. В реальных же условиях эксплуатации система будет подвержена сбоям, некоторые из них могут стать опасными.

Уровень помех, при котором наблюдается формирование ложных сигналов управления, зависит от большого числа факторов (типа аппаратуры, взаимного расположения блоков, температуры и т.д.). Поэтому для определения необходимого уровня помех, вызывающих сбои в аппаратуре, необходимо проводить исследования уровня помехозащищенности устройств и систем железнодорожной автоматики [14].

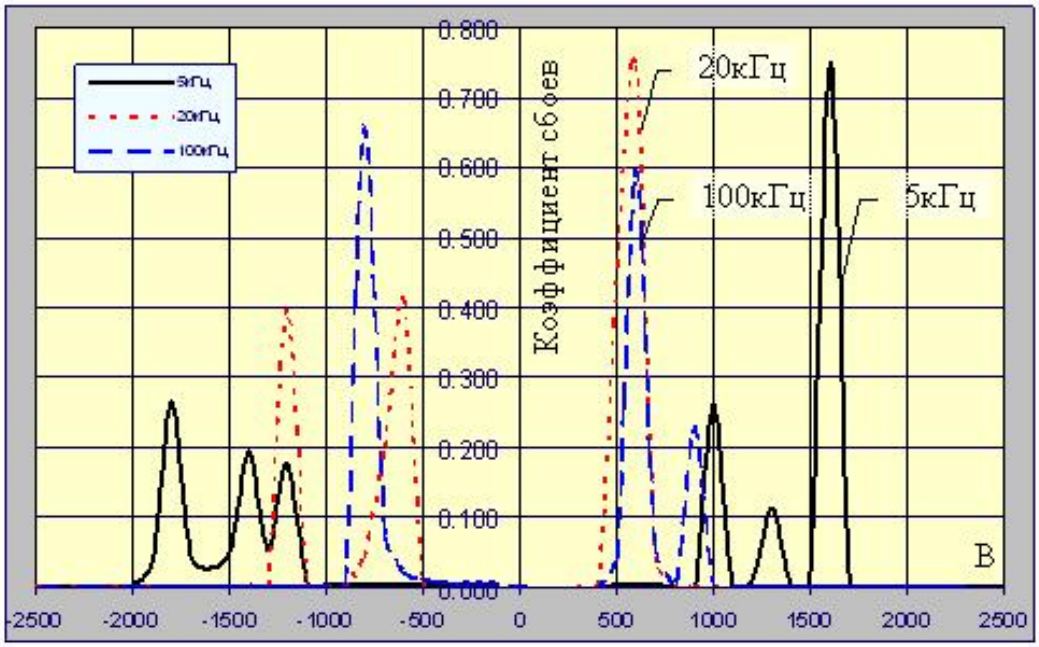

Рис. 4. Зависимость сбоев манипулятора «мышь» компьютеров промышленного исполнения РАС-106, от амплитуды напряжения при различных частотах

Поэтому особенностью проведения испытаний в лаборатории «БЭМС ТС» является комплексный подход к проведению испытаний на функциональную безопасность при воздействии электромагнитных помех.

В этом случае проводится исследование помехозащищенности технических средств испытываемой системы. Исследования проводятся на всем диапазоне возможных изменений параметров электромагнитных помех, в том числе между значениями, соответствующими заданным степеням жесткости.

По результатам исследований определяются параметры помех, вызывающих сбои в нормальном функционировании системы.

После этого проводятся испытания на безопасность при воздействии электромагнитных помех с определенными ранее параметрами.

Выводы

Обзор представленных методов и средств проведения доказательства безопасности микроэлектронных схем на безопасность позволяет сделать следующие выводы:

– ввиду высокой сложности микроэлектронных схем, значительного объема выполняемых расчетов и моделирования анализ проводится 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, каких как КИИБ, СМ-ДЭС или аналогичных программных продуктов.

Библиографический список

1. ГОСТ 27.301-95. Надежность в технике. Расчет надежности. Основные положения [Текст].
2. ГОСТ Р 51901.5-2005. Менеджмент риска. Руководство по применению методов анализа надежности [Текст].
3. ГОСТ Р 51901.13-2005 (МЭК 61025:1990). Менеджмент риска. Анализ дерева неисправностей [Текст].
4. ГОСТ Р 51901.14-2005 (МЭК 61078:1991). Менеджмент риска. Метод структурной схемы надежности [Текст].
5. ГОСТ Р 51901.15-2005. Менеджмент риска. Применение марковских методов.
6. РТМ 32 ЦШ 1115482.02-94. Безопасность ЖАТ. Методы расчета показателей безотказности и безопасности СЖАТ [Текст].
7. Жаднов, В. В. Современные проблемы автоматизации расчетов надежности [Текст] / В. В. Жаднов, И. В. Жаднов, С. Н. Полесский // Надежность. – 2007. – № 2 (21). – С. 3-12.
8. Викторова, В. С. Анализ программного обеспечения моделирования надежности и безопасности систем [Текст] / В. С. Викторова, А. С. Степанянц // Надежность. – 2006. – № 4 (19). – С. 46-57.
9. Сертификация и доказательство безопасности систем железнодорожной автоматики / под редакцией Вл. В. Сапожникова. – М.: Транспорт, 1997. – 288 с.
10. Шевченко, Д. Н. Моделирование надежности систем методом FTA: новые возможности [Текст] / Д. Н. Шевченко // Современные информационные компьютерные технологии: Материалы междунар. конференции, сборник научных статей. Ч. 2. – Гродно, 2008. – С. 154–157.
11. Харлап, С. Н. Особенности применения PSpice при моделировании неисправностей в микроэлектронных схемах [Текст] / С. Н. Харлап, А. А. Королев, О. А. Шмыговская // Проблемы проектирования и производства радиоэлектронных средств: Материалы V Междунар. науч. конф. (Новополоцк, 29–30 мая 2008 г.). – Новополоцк, 2008. – С. 83–86.
12. Харлап, С. Н. Комплекс для проведения имитационных испытаний микропроцессорных систем железнодорожной автоматики на функциональную безопасность [Текст] / С. Н. Харлап // Ресурсосберегающие технологии на железнодорожном транспорте: Материалы Всероссийской науч.-технич. конф. с международным участием. – Красноярск, 2005. – С. 188-193.
13. Бочков, К. А. Влияние наносекундных импульсных помех на безопасность функционирования компьютерных систем управления движением поездов [Текст] / К. А. Бочков, С. Н. Харлап, А. В. Логвиненко // Безопасность движения поездов: Тр. науч.-практич. конф. – Москва, 2002. - С. 28.
14. Бочков, К. А. Методы определения параметров опасных помех при проведении исследовательских испытаний [Текст] / К. А. Бочков, С. Н. Харлап, А. В. Логвиненко // Испытания систем ж.-д. автоматики и телемеханики на безопасность и электромагнитную совместимость: Тр. II-го Междунар. семинара. – Гомель, 2003. – С. 42-54.

Ключевые слова: функциональная безопасность, железнодорожная автоматика, микроэлектронные системы, программные средства.

Ключові слова: функціональна безпека, залізнична автоматика, мікроелектронні системи, програмні засоби.

Key words: functional safety, automatic on railway transport, microelectronic systems, software tools.

Поступила в редколлегию 16.02.2011.
Принята к печати 21.02.2011.