УДК 656.25+06

СПЕЦИФИКА РАЗРАБОТКИ УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ В СООТВЕТСТВИИ С СОВРЕМЕННЫМИ СТАНДАРТАМИ И МЕТОДЫ ПОВЫШЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В. А. КАНДАЛОВ, Ю. Э. ПОНОМАРЕВ, В. В. КАМЕНСКИЙ
Ростовский государственный университет путей сообщения, Российская Федерация

Стандарты ГОСТ Р МЭК 61508 и IEC 61508 являются базовыми для Российских и Европейских стандартов, определяющих порядок разработки устройств, к которым предъявляются требования функциональной безопасности. На рисунке 1 представлены требования к устройствам железнодорожной автоматики и телемеханики в разрезе программной и аппаратной части, предъявляемые общими и отраслевыми стандартами.

Рисунок 1 – Требования к аппаратной и программной части устройств

Согласно стандартам ГОСТ Р МЭК 61508 и IEC 61508 отказы делятся на 2 типа: систематические и случайные. Систематические отказы определяются ошибками спецификации, проектирования, кодирования программного обеспечения; защита от них строится средствами организации жизненного цикла, к которым относятся верификация всех этапов жизненного цикла на соответствие требованиям и валидация (валидационное тестирование) конечного продукта. Случайные отказы рассчитываются как вероятности выхода из строя аппаратных средств, защита от них как правило определяется архитектурными решениями. По стандартам все методы можно разделить на две группы: организационные и технические. К организационным методам относятся: реализация жизненного цикла, применение стандартов кодирования, контроль производства аппаратных средств. К техническим методам относится: разнообразие или диверсность, резервирование, защита от окружающих воздействий, независимость и разделение компонентов, самодиагностика.

Основные организационные методы защиты от систематических ошибок описаны в приложениях ГОСТ Р МЭК 61508. В качестве примера рассмотрим систематическую составляющую программного обеспечения. При написании программного кода следует уделить большое внимание правилам кодирования и стандартам, используемым при кодировании. Известным стандартом при программировании на языке «СИ» является «MISRA-C», его применение улучшает безопасность системы. При этом существуют статические анализаторы, способные проверять исходные тексты программ на соответствие правилам «MISRA-C». Таким образом, использование мирового стандарта «MISRA-C» при разработке программного обеспечения совместно со статическим анализатором кода существенно повышает стойкость кода к систематическим отказам. Частичного диверситета программного обеспечения можно достигнуть за счет применения различных алгоритмов разработки ПО. Полный диверсистет программного обеспечения достигается только тогда, когда имеются две различные спецификации требований на программное обеспечение, разные команды программистов, разные средства программирования устройств при производстве т. е. данные программы должны быть абсолютно разными и процесс программирования устройств тоже должен быть разным. Также при разработке программных средств необходимо защититься от ошибок инструментальных средств. Самым критичным ПО с точки зрения инструментальных средств являются компилятор и линкер. Разнообразия инструментальных средств можно достигнуть, используя компиляторы «ARMCC» и «GCC». При этом некоторые версии

«ARMCC» имеют сертификацию TUV на соответствие SIL-3 согласно IEC 61508, а «GCC» успешно применяется при разработке ПО беспилотных летательных аппаратов и имеет открытые исходные коды, что позволяет однозначно определить поведение инструментального средства. Как видно из таблицы 1, при генерации кода компиляторами «ARMCC» и «GCC» микроконтроллеры используют различные рабочие регистры и команды в разной последовательности, что также уменьшает вероятность отказов по общей причине (Common Cause Failure, CCF).

Таблица 1 – **Сравнение кодов сгенерированных компиляторами**

Команда на языке «СИ» (ISO/IEC 9899) : MDR_PORTE->CLRTX =0x0040	
«GCC»	«ARMCC»
LDR r3, [pc, #20]	MOVS r0,#0x40
MOVS r2, #64 ; 0x40	LDR r1,[pc,#16] ; @0x0000072C
STR r2, [r3, #36]	STR r0,[r1,#0x24]

Рассмотрим методы защиты от случайных ошибок на примере устройства, управления электромагнитным реле, представленного на рисунке 2. Для того чтобы определить методы защиты, необходимо выявить опасные отказы оборудования. Как известно, реле управляется подачей напряжения на его обмотку, в этом случае опасным отказом для данного устройства будет несанкционированное появление напряжения, достаточного для срабатывания реле. Данное устройство строится на архитектуре 2 из 2.

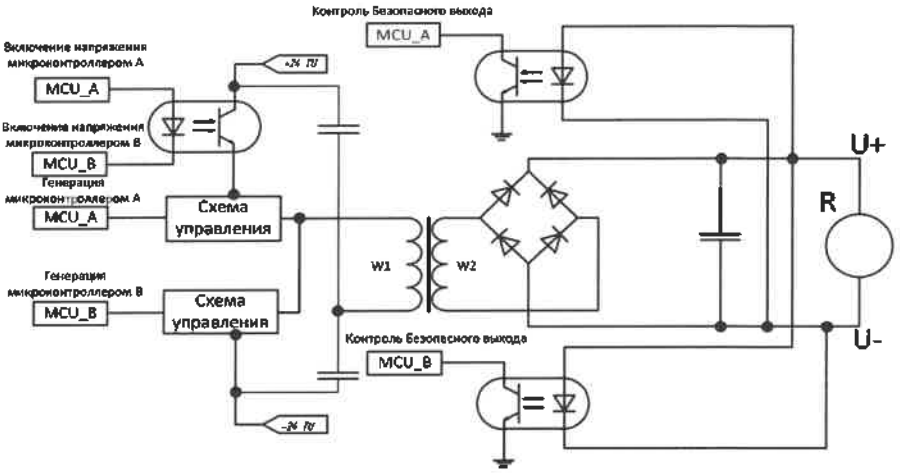

Рисунок 2 – Схема безопасного сопряжения

Опасный отказ возможен только в случае, если одновременно произойдут 4 отказа:

1) включается напряжение питания «+24 TU» на выходе генератора;

2) MCU_A генерирует последовательность импульсов на выходе;

3) MCU_B генерирует последовательность импульсов на выходе;

4) система контроля выходного напряжения не работает и не производит отключение нагрузки. Вероятность того, что одновременно произойдут все 4 события является крайне низкой.

Таким образом, в качестве методов повышения функциональной безопасности рекомендуется применять:

1) диверсификацию программно-аппаратных средств;

2) самодиагностику всех ресурсов микроконтроллеров (ОЗУ, ПЗУ, АЛУ, рабочие регистры и т. д.), а также узлов устройства;

3) снижение параметров элементов схем относительно предельных значений (De-rating) для обеспечения лучших эксплуатационных характеристик и снижения вероятности отказов.

Все перечисленные методы могут быть использованы при разработке устройств железнодорожной автоматики и телемеханики.

Список литературы

1 **Долгий, А. Г.** Система Диспетчерского контроля и управления движением поездов «ДЦ-ЮГ с РКП» / И. Д. Долгий, А. Г. Кулькин, 2010. – 468 с.

2 Гибридная система централизации стрелок и светофоров / И. Д. Долгий, А. Г. Кулькин, 2012. – 388 с.

Таким образом, интеграция предложенного метода графо-функционального моделирования с прикладным пакетом EPlan позволяет формализовать процесс постановки задач разработчикам аппаратного и программного обеспечения. Это делается путем сочетания функциональных вершин с компонентами проектируемой системы и соответствующими им интерфейсными окнами. Аналогичные подходы могут быть применены к другим системам САЕ или САПР с учетом специфики таких систем.

УДК 656.25

ПОДХОД К АВТОМАТИЗАЦИИ АНАЛИЗА ВЛИЯНИЯ ОТКАЗОВ НА ФУНКЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

В. Л. КАТКОВ
Белорусский государственный университет транспорта, г. Гомель

Постоянное развитие и исследование в области железнодорожной автоматики и телемеханики (ЖАТ) ведет к появлению новых сложных технических систем и электронных устройств. Современные тенденции развития ЖАТ – это повсеместное внедрение информационных технологий, переход к цифровым системам, объединение возможностей различных устройств и другое, но неизменным остается требование к обеспечению безопасности и надежности данных систем. Обязательным требованием до внедрения нового устройства в эксплуатацию является его анализ на предмет поведения при возникновении отказов.

Отказ – нарушение работоспособности объекта, при котором система или элемент перестают выполнять целиком или частично свои функции. Неконтролируемые отказы недопустимы в устройствах ЖАТ. Необходимо точно знать, к каким последствиям приведет тот или иной отказ, чтобы предвидеть сбой системы и внести дополнительные меры для его исключения.

Научно-исследовательская лаборатория «Безопасность и ЭМС технических средств» БелГУТа проводит научно-техническую экспертизу и испытания на безопасность функционирования, электромагнитную совместимость и поиск опасных отказов в микроэлектронных и компьютерных системах управления ответственными технологическими процессами, в том числе в системах железнодорожной автоматики и телемеханики.

Существует несколько методов проведения анализа последствий отказов:

– техническая экспертиза предполагает выполнение анализа безопасности функционирования человеком-экспертом;

– лабораторные испытания образцов устройства предполагают физическое внесение отказов элементов в устройство с последующей проверкой правильности функционирования;

– имитационное моделирование предполагает создание модели реального объекта и проведение обязательных испытаний на данной модели посредством воспроизведения на ЭВМ (имитации) процесса функционирования исследуемой системы.

В настоящее время сложность разрабатываемых схем увеличилась настолько, что применение лишь первого или второго из вышеперечисленных методов не целесообразно: например, человек-эксперт не сможет точно описать изменение формы сигналов после отказа внутри цифровой микросхемы, а создание лабораторного стенда с последующим внесением отказов значительно повысит трудоемкость и стоимость проведения испытания.

Оптимальным решением является компьютерное имитационное моделирование. Имитационная модель в этом случае замещает материальный объект. Модель всегда проще объекта. Она отражает только некоторые его свойства, необходимые для проведения определенного анализа. Стоит упомянуть, что разработка и исследование имитационной модели невозможны без предварительного анализа электронной схемы, тем самым выполняется первый метод проведения анализа последствий отказов – человек, выполняющий моделирование, проводит экспертную оценку функциональных блоков устройства, анализирует предоставленную документацию. Тем самым, даже не приступив непосредственно к созданию имитационной модели, может быть обнаружен критический момент в анализируемой схеме.

Сегодня компьютерное имитационное моделирование является важнейшей частью при проведении анализа последствий отказов электронных устройств. Это обусловлено следующими причинами: