В качестве решения данной проблемы предлагается разработать механизм обработки результатов моделирования, который будет анализировать выходные сигналы микроконтроллера и на основе заданных критериев поведения сигнала распознавать и классифицировать тип моделируемого отказа. Для разработки данного программного обеспечения требуется формализовать критерии различных типов отказов и представить их в форме, удобной для машинной обработки.

Критерии опасных (защитных) отказов представляют собой набор условий, при выполнении которых возникает опасный (защитный) отказ. Для формализации данных критериев требуется перейти от набора условий, описанных в технической документации к системе, к конкретным электрическим параметрам выходных сигналов моделируемого устройства. Однако критерии опасного и защитного отказов не охватывают все возможные состояния выходных сигналов. Выделяют еще необнаруживаемые (маскируемые) отказы, при возникновении которых параметры выходных сигналов изменяются незначительно, что не приводит к изменениям в функционировании объекта управления. Кроме того, возможны ситуации, когда требуется более глубокое исследование объекта управления, которое выполнить автоматически не представляется возможным. Это может быть связано, например, с изменением формы выходного сигнала при обрыве выходного конденсатора. В этом случае окончательное решение по классификации отказов должен принимать человек.

Авторами выполнен анализ основных способов задания критериев отказов. Оказалось, что все многообразие критериев можно описать с помощью относительно небольшого перечня типовых условий:

1) наличие импульсных сигналов на одном или нескольких выводах микроконтроллера;

2) изменение уровня сигнала в указанном временном диапазоне;

3) наличие синфазных/парафазных сигналов на нескольких выводах микроконтроллера;

4) задержка при изменении уровня сигнала (задержка на переключение для работы с релейными схемами);

5) сопоставление уровней сигналов с эталонным значением;

6) наличие сформированного сигнала определенной длительности.

При автоматической проверке на соответствие критериям отказов необходимо придерживаться следующего алгоритма анализа:

1 Выполняется проверка критериев опасного отказа. Если хотя бы одно условие выполняется, то делается вывод о наличии в схеме опасных отказов.

2 Если ни одному из критериев опасного отказа выходные сигналы схемы не соответствуют, то выполняется проверка критериев защитного отказа. Если хотя бы одно условие выполняется, то делается вывод о том, что данный отказ является защитным.

3 Если ни одному из критериев опасного и защитного отказов выходные сигналы схемы не соответствуют, то выполняется проверка критериев маскируемого отказа. Если все критерии выполняются, то делается вывод о том, что данный отказ является маскируемым, в противном случае отказ считается неклассифицируемым и подлежит ручному анализу.

Использование программного обеспечения на основе предложенного алгоритма значительно ускорит процесс выполнения анализа результатов моделирования программного комплекса КИИБ, а также позволит избежать ряд ошибок, связанных с человеческим фактором. Предложенный перечень критериев для классификации отказов позволяет с большой достоверностью определить часть отказов автоматически, что значительно сокращает необходимость в ручном анализе данных для неклассифицируемых отказов.

УДК 004.052.2

МЕТОД ВЗАИМНОЙ ПРОВЕРКИ АКСИОМАТИЧЕСКИХ БАЗИСОВ

С. Н. ХАРЛАП, Б. В. СИВКО
Белорусский государственный университет транспорта, г. Гомель

К современным системам, критичным к безопасности, предъявляются повышенные требования по надежности и безопасности функционирования, для выполнения которых необходимо улучшать показатели отказоустойчивости. Для обеспечения соответствующего качества длительно эксплуатируемых устройств необходимо проводить дополнительные мероприятия, которые позволят создать системы, способные к обнаружению отказов, что необходимо для исключения их накопления.

После выявления отказов выполняются действия согласно применяемой стратегии безопасности, например переход в безопасное состояние или запуск процесса самовосстановления.

В настоящее время нет единого подхода, позволяющего выполнить обнаружение отказов для любых систем, и поэтому актуальным является разработка соответствующих эффективных методов и средств. В докладе рассматривается решение с помощью метода взаимной проверки аксиоматических базисов.

Метод основывается на аксиоматико-базисном подходе, в рамках которого выбираются два или более диверситетных аксиоматических базиса, и в дальнейшем реализуются процедуры их взаимной проверки. Другими словами, утверждения одного базиса проверяются на основе функциональности, опирающейся на другой базис. Это дает такое качество, что в случае отказа происходит нарушение одного из базисов, а другой базис остается в работоспособном состоянии и может проверить истинность первого базиса. Как следствие, метод предоставляет надежный и формально верифицируемый способ диагностики.

Во время разработки отказоустойчивой системы по рассматриваемому методу необходимо выполнять ряд мероприятий, в которые входят: выбор диверситетных базисов, доказательство их диверситета, определение общих утверждений базисов для исключения отказов по общей причине, верификация общего базиса вне рассматриваемой теории и др. Как правило, данные решения зависят от рассматриваемой системы, и особенности их применения рассматриваются в докладе.

В настоящее время оценка эффективности метода проведена с помощью имитационного моделирования. В качестве инструмента моделирования применялся КИИБ (комплекс имитационных испытаний на безопасность), который позволяет проводить имитационные испытания на функциональную безопасность в соответствии с IEC 61508, EN 50126, ОСТ 32.146 микропроцессорных систем управления ответственными технологическими процессами. С помощью КИИБ вносились различные отказы, которые могли повлиять на функционирование, и в дальнейшем анализировалось поведение системы. Таким образом, на практике было отработано и подтверждено, что с помощью метода взаимной проверки аксиоматических базисов возможна разработка и верификация безопасных и отказоустойчивых систем, а также целенаправленное и формализованное повышение отказоустойчивости посредством усиления базиса.

Опыт разработки и верификации показал, что метод может быть применен с минимальными затратами к широкому классу систем без предъявления специфичных требований. Также метод позволяет формализованно доказать, что система обладает заданным качеством. Таким образом, с помощью метода взаимной проверки аксиоматических базисов можно выйти на новый уровень формализации и качества в разработке и верификации отказоустойчивых и безопасных систем.

В докладе рассматриваются основные положения метода, его особенности, опыт применения и результаты имитационных испытаний.

УДК 656.25

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ РЕЛЬСОВЫХ ЛИНИЙ ДЛЯ ПЕРЕДАЧИ СИГНАЛОВ ТЕЛЕМЕХАНИКИ

В. И. ШАМАНОВ
Московский государственный университет путей сообщения (МГУПС (МИИТ), Российская Федерация

Устойчивость работы автоматической локомотивной сигнализации (АЛС) и рельсовых цепей (РЦ) на электрифицированных участках железных дорог лимитируется, прежде всего, уровнем помех от тяговых токов. На железных дорогах России количество сбоев АЛС в расчете на один миллион пробега у электровозов в 40–70 раз больше, чем у тепловозов на участках с автономной тягой. При электротяге переменного тока сбоев больше в среднем в 1,7 раза по сравнению с участками, электрифицированными на постоянном токе. Подобная картина наблюдается и на магистральных железных дорогах Казахстана.

Сбои ухудшают безопасность движения поездов, повышают психофизиологическую нагрузку на локомотивные бригады, увеличивают расходы в хозяйстве автоматики и телемеханики, а также в хозяйстве пути на поиск и устранение причин сбоев.