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

КИИБ позволяет контролировать следующие характеристики:

– наличие одиночных и кратных неисправностей технических средств, приводящих к нарушению функциональной безопасности системы;

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

– возможность накопления отказов заданной кратности во внутренней структуре.

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

Существующая версия комплекса имитационных испытаний КИИБ позволяет выделить следующие недостатки, затрудняющие проведение испытаний систем на базе разработанной универсальной модели микроконтроллера:

– недостаточная эффективность средств отладки моделей;

– жесткая ориентация на группы микроконтроллеров, что требует переработки комплекса при моделировании нового микроконтроллера;

– невозможность распределенных вычислений, что снижает производительность.

Для их устранения требуется доработать текущую версию комплекса КИИБ:

1) переработать стандартный внешний интерфейс;

2) доработать модуль тестирования с целью повышения универсальности;

3) переработать визуальные модели ручной отладки и автоматизированного тестирования;

4) реализовать распределенное вычисление при проведении испытаний.

Переработанная организация комплекса позволит обеспечить высокую скорость моделирования при использовании различных интерфейсов для ручной отладки и автоматизированного тестирования; улучшить гибкость системы при помощи повышения универсальности; реализовать параллельное проведения испытаний на нескольких компьютерах.

УДК 656.25

АВТОМАТИЗАЦИЯ АНАЛИЗА РЕЗУЛЬТАТОВ ИМИТАЦИОННЫХ ИСПЫТАНИЙ МИКРОПРОЦЕССОРНЫХ СИСТЕМ НА ФУНКЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ

С. Н. ХАРЛАП, Д. С. САВЕНОК

Белорусский государственный университет транспорта, г. Гомель

При проектировании и разработке систем, критичных к безопасности, особое внимание уделяется составлению доказательства безопасности. Одним из этапов доказательства безопасности являются имитационные испытания (моделирование) аппаратной и программной частей разрабатываемой системы. Для этих целей в ИЛ «БЭМС ТС» БелГУТа разработан программный комплекс для проведения имитационных испытаний микропроцессорных систем железнодорожной автоматики на функциональную безопасность (КИИБ).

Особенностью данного комплекса является имитация отказов в программной модели, полностью реализующей поведение микроконтроллера, и анализ работы неисправного микроконтроллера с загруженным в него программным обеспечением, которое будет использоваться в процессе эксплуатации. Учитывая значительное число моделируемых отказов, проведение испытаний и, особенно, анализ полученных результатов требует длительного промежутка времени.

Результаты моделирования программного комплекса КИИБ предоставляются пользователю в виде графиков выходных сигналов с портов имитируемого устройства для каждого из испытаний. Анализ результатов работы моделируемого устройства заключается в классификации внедренного в модель отказа на основе критериев, установленных в технической документации к системе. Поэтому возникает проблема автоматизации анализа результатов работы имитируемого устройства, так как ручной анализ даже при моделировании небольшого числа отказов приводит к большим временным затратам на обработку информации. Кроме того, при ручном анализе больших объемов данных возрастает вероятность некорректной классификации отказа, связанная с ослаблением внимания человека.

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.