ПРОБЛЕМЫ АВТОМАТИЗИРОВАННОГО АНАЛИЗА РЕЗУЛЬТАТОВ ИМИТАЦИОННЫХ ИСПЫТАНИЙ НА ФУНКЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ МИКРОПРОЦЕССОРНЫХ СИСТЕМ

Д. С. Савенок, С. Н. Харлап
Кафедра «Микропроцессорная техника и информационно-управляющие системы», электротехнический факультет, факультет магистерской подготовки и профориентации, Белорусский государственный университет транспорта
Гомель, Республика Беларусь
E-mail: savenokds@gmail.com

В данной статье рассмотрены особенности анализа результатов имитационных испытаний на функциональную безопасность. Произведен подбор критериев, основанных на характеристиках выходных сигналов электронных устройств, для автоматизированной классификации имитируемых отказов в программного комплекса КИИБ.

Введение

При проектировании и разработке систем, критичных к безопасности, особое внимание уделяется этапу составления доказательства безопасности. Для этого проводят несколько независимых друг от друга процедур, одной из которых являются имитационные испытания (моделирование) аппаратной и программной части разрабатываемой системы. Существующие программные продукты не позволяют производить моделирование поведения программируемых элементов, входящих в состав системы, в частности, микроконтроллеров и микропроцессоров, при возникновении в них отказов. Поэтому для решения данной проблемы в ИЛ «БЭМС ТС» БелГУТа разработан программный комплекс для проведения имитационных испытаний микропроцессорных систем железнодорожной автоматики на функциональную безопасность (КИИБ)[1].

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. Таким образом при каждом внедрении одного или нескольких отказов в модель микроконтроллера требуется провести имитацию его работы. При этом количество проводимых испытаний резко возрастает и анализ полученных результатов требует длительного промежутка времени.

Методы анализа результатов испытаний

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.

На основании перечисленных выше факторов возникает проблема анализа результатов работы имитируемого устройства. Так как в процессе работы микроконтроллера в составе системы управления на его выходах формируются управляющие сигналы, обладающие определенными характеристиками, то ручной анализ каждого из выходных сигналов даже при моделировании небольшого числа отказов приводит к большим временным затратам на обработку информации. В добавок к этому, при ручном анализе больших объемов данных возрастает вероятность некорректной классификации отказа, связанная с ослабления внимания пользователя.

В качестве решения данной проблемы предлагается разработать механизм обработки результатов моделирования, который будет анализировать выходные сигналы микроконтроллера и на основе заданных критериев поведения сигнала будет 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.

Формализация критериев распознавания отказов

Критерии опасных отказов представляют собой набор условий, по выполнению которых возникает опасный отказ и в системе нарушаются работоспособное и защитное состояние. Для формализации данных критериев требуется перейти от набора условий, описанного в технической документации к системе, к конкретным электрическим параметрам выходных сигналов моделируемого устройства.

Произведем формализацию критериев опасного и защитного отказов на примере

устройства включения исполнительных реле (см. рис. 1).

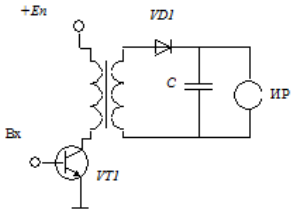

Рис. 1 – Устройство включения исполнительных реле

При поступлении импульсов на вход схема должна формировать на выходе напряжение, достаточное для включения реле. При отсутствии импульсов - реле должно выключаться. Критерии опасного отказа для этой схемы формулируется следующим образом: - Реле не должно включиться при отсутствии на входе импульсов. - Реле должно выключиться при прекращении поступления импульсов в течение времени t, равному задержке на выключение. Необходимо от словесного описания критериев перейти к условиям, связывающим электрические и временные параметры входных и выходных сигналов. Примерами таких условий для данного примера могут быть следующие выражения: - при отсутствии на входе импульсов амплитудой от 0 до 2 В напряжение на выходе не должно превышать 16 В (напряжение включения реле) в течение времени 10 мс (задержка на включение реле); - при прекращении формирования импульсов на входе схемы в течение времени 20 мс (задержка на выключение) напряжение на выходе схемы должно снижаться до 5 В (напряжение выключения реле). Аналогично можно описать критерии защитных отказов схемы. Однако критерии опасного и защитного отказа 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:

- наличие импульсных сигналов на одном или нескольких выводах микроконтроллера;
- изменение уровня сигнала в указанном временном диапазоне;
- наличие синфазных/парафазных сигналов на нескольких выводах микроконтроллера;
- задержка при изменении уровня сигнала (задержка на переключение для работы с релейными схемами);
- сопоставления уровней сигналов с эталонным значением;
- 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.

Заключение

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.

1. Бочков К.А., Харлап С.Н., Шевченко Д.Н. Методы и средства доказательства функциональной безопасности микроэлектронных систем железнодорожной автоматики // Електромагнітна сумісність та безпека на залізничному транспорті/Науково-технічний журнал. – Днепропетровск, 2011. №2. – С.73-81.