Для оценки корректности программ применяется метод функционального тестирования по критериям:

1) проверка всех классов входных данных, когда тест должен содержать по одному представителю из каждого класса;

2) проверка всех классов выходных данных, когда при исполнении тестовых примеров должно быть получено по одному представителю из каждого класса.

Тестовая последовательность (*ABCD*) представлена в таблице 1.

Таблица 1 – **Тестовая последовательность**

№	Входные значения				Ожидаемый результат
	A	B	C	D	Y
T1	**0**	**1**	**0**	**1**	**1**
T2	**1**	**0**	**1**	**0**	**0**

Предположим, что при разработке программ были допущены ошибки. Статистическая вероятность возникновения ошибок в программном обеспечении составляет примерно от 2 до 15 ошибок на 1000 строк кода. Для реализации указанных версий ПО объем кода составляет не более 50 строк, поэтому можно предположить, что вероятность ошибки составит не менее 0,1. Типы ошибок определены экспертно, основываясь на том, что основными причинами ошибок являются невнимательность человека при создании программы и использование неисправных аппаратных средств или некорректно работающих программных инструментальных средств. Рассмотрены следующие типы ошибок:

1) невыполнение (пропуск) инверсии логической переменной;

2) преобразование одной логической операции в другую (например AND в OR и обратно);

3) неверное значение флага сравнения результатов (при выполнении операций сравнения в методе бинарных программ);

4) невыполнение (неполное выполнение) сдвига при формировании адреса в методе адресных переходов.

При оценке версий ПО с помощью EL-модели учитывались только версии программ, наличие ошибок в которых не обнаруживалось тестами.

Для указанных условий были рассчитаны вероятности формирования программами ошибочных результатов. В соответствии с методикой были получены следующие результаты.

Вероятность того, что случайно выбранная программа для случайно выбранного входного значения отработает ошибочно, составляет $Q_1 = 0{,}013$.

Если использовать две случайно выбранные версии с последующим сравнением результатов, то вероятность ошибочного выходного воздействия для случайно выбранного входного значения составляет $Q_2 = 0{,}0006$.

Если же использовать предположение о полной независимости отказов для двух каналов, то это даст более низкую вероятность отказа системы $Q_3 = 0{,}0002$.

Таким образом, результаты исследований подтвердили тезис о том, что полная независимость отказов даже для диверситетных версий ПО не может быть достигнута, т. е. оценку безопасности ПО невозможно получить просто из факта наличия диверситета: нельзя утверждать, что если одна система имеет вероятность опасного отказа λ, то диверситетная система будет иметь вероятность опасного отказа равную λ^2.

УДК 656.25

УРОВНИ ФОРМАЛИЗАЦИИ ФУНКЦИИ БЕЗОПАСНОСТИ ПРИ ВЕРИФИКАЦИИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПОЕЗДОВ

С. Н. ХАРЛАП, Б. В. СИВКО

Белорусский государственный университет транспорта, г. Гомель

Микропроцессорные системы железнодорожной автоматики и телемеханики (СЖАТ) используются на железнодорожном транспорте, где главным аспектом является безопасность движения поездов. К таким системам предъявляются повышенные требования по безопасности, надёжности и

отказоустойчивости, и для обеспечения надлежащего уровня функционирования необходимо проводить дополнительные мероприятия, одним из которых является доказательство функциональной безопасности.

При выполнении процедуры доказательства безопасности необходимо документально подтвердить выполнение всех функций безопасности проверяемой системы с заданным уровнем полноты безопасности (УПБ). Для этого необходимо пройти несколько этапов:

1) сформировать перечень функций безопасности, определить критерии опасного и защитного отказа системы в целом;

2) выполнить трассировку системных требований до каждой функции безопасности, определить критерии опасного и защитного отказа для каждой функции;

3) определить способ подтверждения соответствия (верификации) каждой функции требованиям функциональной безопасности;

4) разработать методики и программы проведения мероприятий по верификации (экспертиза, тестирование, испытания);

5) выполнить мероприятия по верификации и оформить отчетные материалы (экспертные заключения, расчеты, протоколы тестирования и испытаний).

Для того, чтобы обеспечить однозначность, достоверность и проверяемость результатов верификации, необходимо выполнить формализацию свойств системы, реализуемых функций и критериев отказов. В частности, без подобной формализации может оказаться невозможным применение формальных методов при подтверждении соответствия. Данная необходимость обусловлена высокими требованиями по показателям безопасности и надёжности систем, связанных с безопасностью движения поездов.

В статье рассмотрены три уровня формализации: неформализованный, формализованный и проверяемый. Первый из них, как правило, является вербальной формулировкой – он абстрактен, удобен при общении и не требует существенных затрат. Так, он используется в нормативных документах (ГОСТ, ПТЭ, ИСИ и др.). Именно неформальный уровень используется на начальных этапах доказательства безопасности, где требования безопасности и критерии отказов обычно оформляются в виде технического задания или спецификации требований. В этом случае используются такие формулировки, как «При замыкании маршрута приема должны проверяться следующие условия: отсутствие установленного встречного поездного или маневрового маршрута на железнодорожный путь …».

Однако при проведении дальнейших работ по верификации требуется частичная или полная формализация требований и критериев отказов, которая устраняет неоднозначности и после её проведения возможно применение некоторой формальной системы во время верификации. Например, при трассировке системных требований возникает потребность в однозначной идентификации каждого требования на различных уровнях иерархии системы. Так, для рассмотренного выше примера можно выделить как минимум четыре уровня иерархии:

[МПЦ_ОСН_УПБ4] – функции безопасности в основном режиме управления;

[ОСН_УПМР_УПБ4] – функция безопасности «Установка поездного маршрута с замыканием секций маршрута и включением разрешающего показания на железнодорожном светофоре»;

[УПМР_ЗПМ_УПБ4] – замыкание поездного маршрута;

[ЗПМ_ОВМ_УПБ4] – отсутствие установленного встречного поездного или маневрового маршрута на железнодорожный путь.

После определения способа подтверждения соответствия выполняется следующий этап формализации, глубина которой зависит от выбранного способа подтверждения. При экспертизе дальнейшая формализация обычно не выполняется, для выполнения расчетов критерии описываются числовыми значениями, а, например, при автоматизированном тестирования критерии отказов описываются в виде булевых выражений. При этом переход к формальному уровню достаточно сложен, неоднозначен, требует согласованной работы разработчика и организации, проводящей экспертизу, поэтому желательно переходить ко второму уровню формализации как можно раньше. Опыт верификации микроэлектронных СЖАТ выявил ряд ситуаций, когда переход к формализованному уровню не представляется возможным. В этом случае решением является формализованное описание свойств рассматриваемого понятия, и далее во время доказательства безопасности делается экспертное заключение.

Формализованный уровень характерен тем, что свойство может быть описано в виде знаков некоторой формальной системы. Так, если на неформализованном уровне свойство определяется, как «При замыкании маршрута приема должно проверяться отсутствие установленного встречного поездного или маневрового маршрута на железнодорожный путь», то на формализованном уровне нужно для конкретной системы описать данное свойство так, чтобы была возможность математически строгой проверки, например, в виде выражений булевой алгебры.

Проверяемый уровень достигается тогда, когда возможно проведение автоматизированного испытания или тестирования для проверки рассматриваемого свойства. Например, проверка зависимостей системы МПЦ, реализованных программным способом, предполагает полный перебор всех возможных технологических ситуаций на станции. Количество таких ситуаций может быть очень большим, а ручная проверка занимать значительное время. Поэтому в таких случаях широко используются системы автоматического тестирования, для успешной работы которых необходима формализация как свойств системы, так и критериев отказов. На практике проверяемый уровень не всегда достижим в полном объеме из-за сложности системы, ограниченности ресурсов для доказательства или других факторов.

Таким образом, формализация является необходимым элементом процессов верификации и доказательства безопасности микропроцессорных систем. При этом надо стремиться обеспечить как можно более высокий уровень формализации, так как это позволяет применять средства автоматизации проведения тестирования и испытаний, повышает достоверность и проверяемость результатов верификации.

УДК 621.391.825

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ГЕНЕРАТОРА ВЫБРОСОВ 1,2/50 ПУТЕМ ИСПОЛЬЗОВАНИЯ УСЛОВИЯ ЭКВИВАЛЕНТНОСТИ ИМПУЛЬСОВ ПОМЕХ

С. И. ХОМЕНКО, И. О. ЖИГАЛИН, В. Л. КАТКОВ, И. В. ЛОГВИНЕНКО
Белорусский государственный университет транспорта, г. Гомель

При проведении испытаний на устойчивость к выбросу напряжения стандарт ГОСТ IEC 61000-4-5-2017 [3] предполагает для 4–5-го класса условий эксплуатации применение генераторов выбросов следующих видов: комбинированный генератор выбросов 1,2/50 мкс и комбинированный генератор выбросов 10/700 мкс. Для 1–3-го классов условий эксплуатации применяется только комбинированный генератор выбросов 1,2/50 мкс.

Испытание генератором 10/700 мкс проводится редко вследствие чего испытательные лаборатории часто не оснащены соответствующим генератором.

Для обеспечения возможности проведения испытаний генератором выбросов 1,2/50 мкс вместо генератора выбросов 10/700 мкс необходимо определить возможность использования генератора выбросов 1,2/50 путем изменения его параметров согласно условию эквивалентности импульсов.

Импульс, формируемый в соответствии со стандартом, представляет собой двухэкспоненциальный импульс с коротким фронтом. Для упрощения вычислений в данном случае существует возможность представления его в виде экспоненциального импульса с параметрами активной длительности и амплитуды, как у импульса генератора выбросов.

Необходимыми и достаточными требованиями для обеспечения эквивалентности воздействия импульсов [1] является выполнение условий одинаковости их активной ширины спектра Δf_1 и Δf_2, а также полных энергий W_1 и W_2:

$$\begin{cases} W_1 = W_2, \\ \Delta f_1 = \Delta f_2. \end{cases}$$

Генератор выбросов позволяет менять только амплитуду импульса, т. е. формировать эквивалентный импульс можно только с соответствующим поправочным коэффициентом к амплитуде $N_{\text{норм}}$.

Определим параметры экспоненциального импульса с активной длительностью 50 мкс эквивалентного экспоненциальному импульсу с активной длительностью 700 мкс.