УДК 004.312.466

С. Н. ХАРЛАП, кандидат технических наук, Б. В. СИВКО, ассистент, Белорусский государственный университет транспорта, г. Гомель

ВЕРИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МИКРОПРОЦЕССОРНОЙ СВЕТООПТИЧЕСКОЙ СВЕТОДИОДНОЙ СИСТЕМЫ

Приведены результаты анализа функциональной безопасности микропроцессорной системы светооптической светодиодной мачтового железнодорожного светофора с помощью доказательства корректности. Показано, что доказательство безопасности программного обеспечения чрезвычайно затруднено в случае, если разработка аппаратно-программного комплекса проводилась без каких-либо специальных правил для выполнения последующей успешной верификации. Произведена апробация разрабатываемых методов для создания программного обеспечения, отвечающего требованиям безопасности и надежности функционирования.

В области систем железнодорожной автоматики и телемеханики (СЖАТ) продолжается процесс перехода (там, где это целесообразно) от релейно-контактной техники к бесконтактной, что связано с развитием и совершенствованием микроэлектронной базы, которая позволяет расширить функциональность оборудования, улучшить эксплуатационные и информационные характеристики, снабдить действующие системы развитым диагностическим оборудованием и т. п. Появляется возможность решать более сложные задачи, которые реализуют большее число функций и, как следствие, состоят из большего числа элементов и блоков [1, 2]. Одним из способов их внедрения в действующие релейные СЖАТ является разработка таких аппаратно-программных комплексов (АПК), которые могут быть использованы в существующих системах без каких-либо доработок или изменений. Микропроцессорная система светооптическая светодиодная мачтового железнодорожного светофора (ССС-200-60) использует данный способ, выполняя требования интерфейсов релейной схемотехники и может быть непосредственно установлена на место лампы действующего светофора [3]. Тем не менее, она входит в состав общего комплекса СЖАТ и, следовательно, должна удовлетворять соответствующим требованиям безопасности. Создание безопасного программного обеспечения для светооптических светодиодных систем актуально, так как сейчас на базе релейных схем решена задача только для устройств с малым удалением от шкафов, а в случае удаленных светофоров одним из предполагаемых вариантов является разработка интеллектуальной микропроцессорной системы [4].

В настоящее время доказательство безопасности функционирования микропроцессорных устройств, используемых на железной дороге, является одной из проблем, для которой не существует единого решения. В связи с этим применяется комплекс подходов, каждый из которых имеет свои достоинства и недостатки, а так как отсутствует единая методика, то идет поиск различных эффективных способов проведения верификации. В лаборатории БЭМС ТС БелГУТа (далее лаборатория) проводятся испытания устройств на безопасность функционирования, и, так как рассматриваемая система микропроцессорная, то имеющееся программное обеспечение (ПО) анализировалось на наличие ошибок. Доказательство корректности являлось одним из способов их поиска и использовалось для верификации готового ПО с целью выяснения соответствия имеющейся спецификации программы и её реализации.

ССС-200-60 имеет в своем составе один микропроцессор, осуществляющий анализ состояния входных линий и установку согласно спецификации выходных воздействий, обеспечивающих уровни напряжений входов светодиодной матрицы, которая реализует основную функцию устройства как светофора. Входную информацию микроконтроллер анализирует посредством аналого-цифровых преобразователей (АЦП), с помощью которых определяется тип входного напряжения (переменное или постоянное) и требуемый режим работы (яркость свечения светодиодов). Выходные управляющие воздействия являются дискретными сигналами, часть которых изменяется во времени, обеспечивая тем самым необходимый уровень среднего значения напряжения. В зависимости от входных состояний светофор обеспечивает три режима яркости: дневной, ночной и светомаскировки. При этом он может работать как с переменным, так и с постоянным входным напряжением и обеспечивать мигание.

Анализ на безопасность функционирования проводился в соответствии с концепцией безопасности для микроэлектронных систем: «Одиночные дефекты аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться с заданной вероятностью при рабочих и тестовых воздействиях не позднее, чем в системе возникнет второй дефект» [5]. Критериями опасных отказов для данной системы являются [6]:

– изменение цветности сигнала на более разрешающую (красный на желтый и другие);

– горение (в том числе и кратковременное) сигнала при отсутствии входного напряжения под действием наводок в линии;

– изменение показания сигнала той же цветности на более разрешающее (желтый на желтый мигающий);

– снижение интенсивности свечения сигнала (переключение на ночной режим вместо дневного);

– поддержание под током огневого реле при погасшем сигнале.

Критерием защитного отказа считается состояние, обеспечивающее обесточивание огневого реле.

Исходя из сформулированных требований рассматриваемая ССС-200-60 должна выполнять корректную установку уровней выходных сигналов, задающих яркость светодиодов исходя из значений входных параметров, что может быть математически точно сформулировано. С другой стороны, система динамична и её поведение во многом определяется временными характеристиками, для выяснения которых необходимо не доказывать выполнение некоторого условия, а вычислять определенные значения параметров функционирования. Например необходимо знать, за какое гарантированное время программное обеспечение выполнит изменение выходных значений параметров в случае изменения входных. В дальнейшем вычисленные значения могут быть использованы для анализа работы комплекса в целом или переданы на экспертную оценку.

Поведение внутренней логики ПО ССС-200-60 зависит в основном от режима работы, задаваемого входным напряжением, которое анализируется с помощью АЦП. Так вычисляется входное напряжение (по нему происходит выбор одного из режимов яркости) и определяется тип напряжения (постоянное или переменное). Правила однозначных переходов в состояния показаны в таблице 1.

Таблица 1 – **Значения входных сигналов в различных режимах**

Тип	Диапазоны входных сигналов АЦП[1)]	Режим светодиодной матрицы, %
~	Более 303	100
~	225–282	40
~	137–169	2
~–[2)]	Менее 170	40
~–	Менее 90	2
–	Более 244	100
–	176–231	40
–	90–167	2
sleep[3)]	Менее 85	0

[1)] Значения уровней АЦП являются внутренними константами и определяются исходя из экспериментальных данных и характеристик комплекса.

[2)] Работа программы при пропадании входного напряжения, во время которого предполагается, что идёт режим мигания.

[3)] Устройство отключено от входных цепей или входное напряжение близко к нулю.

ПО ССС-200-60 имело среднюю сложность для верификации доказательством правильности (около 700 строк ассемблерного кода), но основными факторами повышенной сложности являлись низкая структурированность (только 30 % кода являлись подпрограммами), смешивание основной логики и получения значений входных параметров, наличие большого числа GOTO-переходов в различные точки программы и, как следствие, создание спагетти-кода [7]. Из-за этого условия безопасности при верификации доказательством правильности были значительно ослаблены, а анализ оказался усложненным.

Наличие каждого дополнительного условного перехода внутрь процедур значительно усложняет анализ и верификацию ПО из-за того, что для выведения предусловий и постусловий с движением сверху вниз и снизу вверх происходит наложение различных контекстов и поведения всего АПК. Аналогичный эффект возникает при смешивании основной логики программы и действий по получению входных параметров, так как при обновлении входных данных происходит изменение контекста выполнения программы.

Ослабление входных условий безопасности отразилось на допущении о времени установки входного сигнала и на верифицируемых диапазонах входных параметров. Первое условие заключалось в том, что система должна переходить в необходимый режим в случае неизменных входных сигналов в течение двух циклов внутренней обработки. Если же входной сигнал не является постоянным, то анализ поведения ПО представляется затруднительным, а работа внутренней логики менее предсказуемой. Второе условие вытекает из-за неоднозначности поведения на смежных диапазонах напряжения. Как можно заметить, в таблице 1 все возможные уровни сигналов АЦП не определены полностью, например, в интервале от 169 до 225 нет однозначного поведения и здесь система может установить как режим 40 %, так и 100 %, поэтому при анализе на безопасность рассматривалось поведение ПО только при попадании уровней сигналов в указанные диапазоны.

Ослабление условий безопасности позволило провести верификацию с использованием доказательства правильности и выявить ряд недостатков рассматриваемого программного решения.

В начале верификации были сформулированы условия безопасности, для описания которых введем следующие определения:

– $U(t)$ – входное напряжение линии АЦП, задающей режим работы;

– $O(t)$ – выходные значения ключей для каждого из режимов (всего в системе имеется шесть выходных ключей, определяющих яркость светодиодной матрицы; здесь же $O(t)$ принимаем как установку всех шести ключей в нужное состояние);

– $f(t)$ – одна из функций $O(t)$ и $U(t)$;

– $R(f(t))$ – режим работы согласно функции $f(t)$;

– T_{max} – максимальное время работы внутреннего цикла;

– $T_ф$ – время неизменности режима работы.

С помощью введенных определений условие безопасности базируется на том, что если устанавливаемый режим не изменяется в течение двух циклов, то есть выполняется следующее условие:

$$\forall(t_1, t_2) \in (t_0 < t_1, t_2 < t_0 + 2T_{max} + T_ф), \quad R(U(t_1)) = R(U(t_2)), \tag{1}$$

где t_0 – начало некоторого рассматриваемого отрезка времени,
тогда должно выполняться следующее условие:

$$\forall t \in (t_0 + 2T_{max} < t < t_0 + 2T_{max} + T_ф), \quad R(O(t)) = R(U(t)). \tag{2}$$

Графически (1) и (2) показаны на рисунке 1.

Рисунок 1 – Условия безопасности выходных ключей ССС-200-60

Таким образом, система при выполнении входных условий перехода в какой-либо режим должна обязательно установить соответствующие режиму выходные значения по истечении двух внутренних циклов ПО.

При анализе внутренний алгоритм был представлен в виде графа с переходами согласно логике Флойда-Хоара [8]. В дальнейшем были определены программные конструкции, которые способны повлиять на условия безопасности. Это позволило установить, как происходит получение входных значений линий АЦП и как возможно изменение выходных значений ключей. Во время верификации состояние системы было представлено в виде объединения двух множеств: внутренних регистров процессора и внешних условий системы.

Верификация проводилась в два этапа:

1) доказательство инициализации и выхода в рабочий режим;

2) проверка выполнения условий безопасности во время постоянной работы в рабочем режиме.

Каждый из этапов разбивался на три последовательные независимые фазы. На первой из них доказывалось, что выполнение программы обязательно достигнет какой-то точки (на первом этапе это точка выхода в рабочий режим, а на втором – точка начала внутреннего цикла). Вторая фаза заключалась в определении выполнения условий безопасности в начале каждого цикла и в момент выхода в рабочий режим. Третья фаза проводилась для расчета временных характеристик работы системы.

Во время верификации на второй фазе для обоих этапов применялось доказательство с использованием предикатов абстракций (*Predicate Abstraction*) [9]. С помощью данного метода были быстро получены простые графы сценариев запуска для различных внешних условий при известном состоянии во время инициализации микроконтроллера, что позволило получить все варианты выхода в рабочий режим. Для второго этапа использование предикатов абстракций стало необходимым в силу низкой структурированности ПО и наличия спагетти-кода, где каждый внутренний GOTO-переход требовал отдельного рассмотрения, во время которого необходимо заново формулировать новые условия предикатов абстракций и определять инварианты внутренних малых циклов.

Для вычисления временных параметров на третьей фазе использовался метод введения переменной времени, изменяющейся при переходе от одной вершины графа переходов по логике Флойда-Хоара к другой согласно тактам выполнения команд микроконтроллера. При анализе больших объемов кода программные структуры (подпрограммы, логические конструкции или отдельные команды низкого уровня) были представлены в виде пары значений (t_{min}, t_{max}), где t_{min} – это минимальное время выполнения рассматриваемой структуры; t_{max} – максимальное. Две программные конструкции, выполняющиеся друг за другом, объединялись так, как показано на рисунке 2.

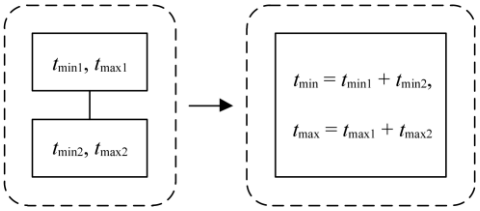

Рисунок 2 – Объединение программных структур для вычисления временных характеристик

Данное объединение является постоянным расширением условий, но, как показала практика, такой оценки в большинстве случаев достаточно для быстрой и эффективной верификации. Полученные на третьей фазе временные параметры уже были вычисленными характеристиками системы, использовались для экспертной оценки и являлись дополнением к предыдущим этапам (например при определении возможных значений T_{max}).

Верификация выявила у рассматриваемой системы ряд недостатков, некоторые из которых неприемлемы с точки зрения безопасности функционирования. Так, одним из результатов было вычисленное время T_{max}, которое в редких случаях могло принимать большие значения, увеличивая время реакции системы до 1,6 секунд по причине наличия ошибок в программной реализации. Например, при переходе светофора из одного из режимов 40 или 100 % по постоянному напряжению в режим по переменному 2 % ПО считает, что это режим мигания, и поэтому находится в ожидании, которое завершается засыпанием микроконтроллера с длительным выходом из него. Такое поведение системы говорит о том, что она может долго реагировать на внешние изменения даже при штатных условиях функционирования, а расчетное время изменения выходных параметров намного больше времени реакции релейных систем, что недопустимо для устройств подобного класса с точки зрения безопасности.

Во время верификации был сделан ряд ослаблений проверяемых условий, которые исключили принцип недоверия, из-за чего рассматривалась работа системы в случае, когда входные сигналы всегда попадают в указанные диапазоны и при этом стабильны (не представляют собой случайный или переменный сигнал). Если в систему изначально не заложены механизмы защиты от внешних ошибочных типов поведения, то правильность работы такой системы доказать либо сложно, либо невозможно из-за того, что условия безопасности при нештатном внешнем поведении не выполняются. Во время проводимой верификации ССС-200-60 было установлено, что ПО может повести себя непредсказуемым образом при переполнении входных значений, получаемых от линий АЦП, когда напряжение превышает

расчетную разрядность. При таком превышении уровень сигнала может быть распознан как пониженный (например 30 В воспринят как 10 В) и светодиоды перейдут в режим дневного света. В данном случае какие-либо утверждения сделать было затруднительно, так как с точки зрения анализа доказать присутствие потенциальной ошибки невозможно и, следовательно, нельзя выдать соответствующее заключение, но при этом имеется вероятность, что ошибка имеет место, доказывать отсутствие которой уже не является задачей лаборатории. В таких случаях делаются рекомендации и АПК дорабатывается таким образом, чтобы доказать отсутствие такого типа ошибок было возможно.

По результатам верификации лабораторией было сделано заключение, что ССС-200-60 не соответствует требованиям ОСТ 32.41–95, ОСТ 32.78–97, ОСТ 32.146–2000 по критерию безопасности функционирования. В дальнейшем рассматриваемое устройство проходило испытания на Горьковской дороге [10]. Были сформулированы рекомендации, представляющие собой конкретные предложения по исправлениям АПК для того, чтобы сделать его работу более корректной и верифицируемой, в частности, изменение ПО таким образом, чтобы отсутствовали самопроизвольные переходы внутрь процедур, имелся гарантированный возврат в начало цикла на любой итерации, присутствовал единый механизм снятия входных и установки выходных параметров. Это позволяет сократить затраты на разработку, сопровождение и верификацию, гарантирует меньшее максимальное время обработки одного цикла и встраивает эффективные механизмы поведения в условиях нештатных ситуаций.

Опыт проведения доказательства корректности показал, что анализ на безопасность чрезвычайно сложен в случае, если АПК к нему не подготовлен. Применение во время разработки некоторого набора правил позволяет сделать систему более надежной, а анализ – более прозрачным и эффективным.

На основе результатов анализа с помощью доказательства корректности предполагается построение набора методов и средств, позволяющих производить более быстрый поиск ошибок и выработать общие правила и рекомендации для разработки безопасных алгоритмов. Выполненное доказательство корректности является апробацией разрабатываемых нами методов, направленных на создание безопасного и надежного ПО, и показывает, что с его помощью возможно проводить поиск ошибок микроэлектронных устройств, вычислять характеристики АПК и предоставлять рекомендации к его улучшению.

Список литературы

1 **Сапожников, В. В.** Какими должны быть микропроцессорные системы железнодорожной автоматики и телемеханики / В. В. Сапожников, Вл. В. Сапожников, Л. И. Борисенко // Автоматика, телемеханика и связь. – 1988. – № 5. – С. 32–34.

2 **Сапожников, В. В.** Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В. В. Сапожников [и др.]; под ред. Вл. Сапожникова. – М. : Транспорт, 1995. – 272 с.

3 Системы светооптические светодиодные мачтовых железнодорожных светофоров ССС 200-60-К, ССС 200-60-Ж, ССС 200-60-3. Доказательство безопасности. – СПб., 2002.

4 **Пусвацет, Ю. Ю.** Светодиодные светооптические системы для удаленных светофоров / Ю. Ю. Пусвацет, Н. Ю. Широков // Автоматика, связь, информатика. – 2010. – № 1.

5 **Бочков, К. А.** Методы обеспечения безопасности в микропроцессорных системах железнодорожной автоматики и телемеханики: учеб. пособие для студентов / К. А. Бочков, С. Н. Харлап; Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2001.

6 Требования безопасности. Светооптические системы светодиодные для железнодорожных светофоров: утв. зам. ЦШ 21.01.2001. – Минск, 2001.

7 **Dijkstra, E. W.** Go to Statement Considered Harmful / E. W. Dijkstra // Communications of the ACM. – 1968. – Vol. 11. – № 3. – 1968. – P. 147–148.

8 **Hoare, C. A. R.** An axiomatic basis for computer programming / C. A. R. Hoare // CACM. – 12(10):576–580, 583. – October 1969. DOI:10.1145/363235.363259.

9 **Graf, S.** Construction of abstract state graphs with PVS / S. Graf, H. Saidi // In Proc. of CAV'1997: Computer Aided Verification. – Vol. 1254 of LNCS. – 1997. – P. 72–83.

10 **Метелев, С. П.** Итоги испытаний светодиодных светофоров и маршрутных указателей / С. П. Метелев // Автоматика, связь, информатика. – 2005. – № 10.

Получено 13.04.2012

S. N. Kharlap, B. V. Sivko. Problems of software verification of the microprocessor light-optical LED system.

The verification results of the microprocessor light-optical LED railway mast traffic light system are published. It is shown that proof of correctness is extremely difficult if the computer appliance has not been prepared to the verification. Testing of the emerging verification technique of developing safety and reliable software is performed.