Методика оценки функциональной надежности компонент программно-аппаратной встраиваемой микропроцессорной системы управления

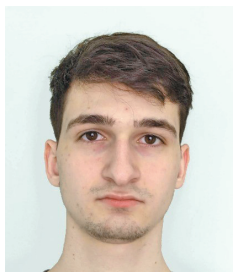
A methodology for evaluating the functional dependability of the components of an embedded software and hardware microprocessor-based control system

Климов С.М.[1], Сосновский Ю.В.[2*],Чачиев Д.Р.[2]
Klimov S.M., Sosnovskiy Yu.V., Chachiev D.R.

[1]*МГТУ им. Н.Э. Баумана, Москва, Россия*
[2]*Физико-технический институт Крымского федерального университета им. В.И. Вернадского, Симферополь, Россия*
[1]*Bauman Moscow State Technical University, Moscow, Russian Federation*
[2]*Physics and Technology Institute, Crimean Federal University named after V.I. Vernadsky, Simferopol, Russian Federation*
**yuri.sosnovskij@yandex.ru*

Климов С.М.

Сосновский Ю.В.



Чачиев Д.Р.

Резюме. Цель. *Выполнить анализ терминологии надежности применительно к встраиваемым программно-аппаратным системам, разработать методику оценки функциональной надежности компонентов программно-аппаратной встраиваемой микропроцессорной системы управления и провести практическую оценку надежности актуальных на сегодняшний день программно-аппаратных компонент уровня встраиваемого компьютера и микроконтроллера для выбора оптимальной структуры системы управления. В качестве объекта управления используется опытный образец медицинского робота, выполняющего функции удержания хирургических инструментов, ранорасширителей по Фараберу и пр. В состав системы робота входит микропроцессорный блок на распространенном одноплатном компьютере, реализующий высокоуровневые функции управления и распознавания голосовых команд, дополнительный микропроцессорный блок для управления сервоприводами и получения входных сигналов, а также исполнительные модули – приводы. Методы. В статье применяются методы анализа библиографических источников, выполнен анализ нерецензируемых сборников документов, ранее закрытых иностранных стандартов и публикаций. Результаты. Представлена методика оценки функциональной надежности компонентов программно-аппаратной встраиваемой микропроцессорной системы управления. Выполнен расчет вероятности безотказной работы программных и аппаратных компонент рассматриваемой системы по статистическим оценкам и по объему кода. Несмотря на различные методы расчета и справочные данные, результаты в целом близки. Также выполнена оценка вероятности безотказной работы программных средств для альтернативной структуры системы управления, когда часть важных функций разделена с дополнительным программно-аппаратным блоком, имеющим более высокий уровень надежности. В данном случае таким блоком является микроконтроллер Atmega32, который будет обеспечивать непосредственное управление работой приводов. Сравнительный анализ результатов показывает, что за счет внедрения дополнительного уровня с частичным распараллеливанием функций и частичным резервированием каналов управления была значительно повышена оценка вероятности безотказной работы системы в заданных условиях. На основании расчетов сформирована структура системы управления с двумя системными уровнями, обладающая высокими значениями вероятности безотказной работы. Заключение. С учетом тенденции к интеграции максимального числа функций в единую микропроцессорную систему, для повышения функциональной надежности предпочтительной схемой является двухуровневое структурное представление функциональной схемы, при котором ключевые задачи в части непосредственной работы с аппаратным окружением перераспределяются в пользу отдельного аппаратного модуля. Кроме того, в рамках встраиваемых систем такой подход часто позволяет выделить нижний системный уровень, работающий в режиме реального времени и верхний системный уровень, отвечающий за высокоуровневые функции, такие как распознавание речи, передачу данных посредством коммуникационных интерфейсов и реализацию функций искусственного интеллекта. Не до конца решенным является вопрос практической оценки надежности встраиваемого программного обеспечения, особенностью которого является отсутствие виртуализации и уровня аппаратной абстракции и, как следствие, тесная взаимосвязь с аппаратной частью и периферией. Очевидно, что*

во время испытаний недостаточно многократно повторять соответствующие испытания, а целесообразно формировать тестовые комбинации из внешних аппаратных воздействий (аномалий сигнального уровня) и программных воздействий на периферию микроконтроллера.

Abstract. Aim. *To analyse the dependability terminology as regards embedded software and hardware systems, to develop a methodology for assessing the functional dependability of the components of embedded software and hardware computer-based control systems, and to conduct a practical assessment of the dependability of the modern software and hardware components of embedded computers and microcontrollers for the purpose of selecting the optimal control system architecture. A prototype medical robot intended for holding surgical instruments, Farabeuf retractors, etc. is used as the controllable object. The robotics system includes a microprocessor unit based on a common single-board computer that implements high-level control and voice command recognition functions, an additional microprocessor unit for controlling servo drives and receiving input signals, as well as the actuating modules, i.e., drives.* **Methods.** *The paper uses reference source analysis, analyses non-peer-reviewed collections of documents, previously restricted foreign standards and publications.* **Results.** *The author presents a method for assessing the functional dependability of the components of an embedded software and hardware control system. The probability of no failure of software and hardware components of the examined system was calculated based on statistical estimates and on the amount of code. Despite the different calculation methods and reference data, the results are generally close. The paper also estimated the probability of no software failure for an alternative control system architecture, whereas a part of important functions is shared with an additional software and hardware unit having a higher level of dependability. In this case, such is an Atmega32 microcontroller that is to directly control the drives. A comparative analysis of the results shows that the additional level with partially parallelised functions and partial control channel redundancy significantly improved the assessment of the system's probability of no failure under predefined conditions. Based on the calculated data, the paper defines a control system architecture with two system levels that has high values of probability of no failure.* **Conclusion.** *Given the trend of growing numbers of functions being integrated within a single microprocessor-based system, improved functional dependability should be achieved through a two-level functional architectural solution, whereas the key tasks in terms of direct interaction with the hardware environment are redistributed in favour of a separate hardware module. Additionally, as regards embedded systems, such an approach often allows defining a lower, real-time system layer and an upper system layer that is responsible for high-level functions such as speech recognition, data communication via interfaces, and artificial intelligence. The matter of practical evaluation of embedded software dependability is not yet completely resolved. Such software is characterised by the lack of virtualisation and a level of hardware abstraction, which, in turn, causes a close relationship with the hardware and peripherals. Obviously, repeating the required tests is not enough. Test combinations should include external hardware effects (signal level anomalies) and software effects on the periphery of a microcontroller.*

Ключевые слова: *программно-аппаратные системы, встраиваемые системы, функциональная надежность.*
Keywords: *software and hardware systems, embedded systems, functional dependability.*

Для цитирования: *Климов С.М., Сосновский Ю.В., Чачиев Д.Р. Методика оценки функциональной надежности компонент программно-аппаратной встраиваемой микропроцессорной системы управления // Надежность. 2025. №1. С. 58-66. https://doi.org/10.21683/1729-2646-2025-25-1-58-66*
For citation: *Klimov S.M., Sosnovskiy Yu.V., Chachiev D.R. A methodology for evaluating the functional dependability of the components of an embedded software and hardware microprocessor-based control system. Dependability 2025;1:58-66. https://doi.org/10.21683/1729-2646-2025-25-1-58-66*

Поступила: *11.10.2024* / **После доработки:** *18.11.2024* / **К печати:** *05.03.2025*
Received on: *11.10.2024* / **Revised on:** *18.11.2024* / **For printing:** *05.03.2025*

Введение

Встраиваемые системы активно развиваются как в сфере гражданского, так и специального назначения. Например, роботизированные ассистенты хирурга, которые помогают выполнять операции точнее и быстрее. В связи с миниатюризацией и удешевлением таких компонент, как система на кристалле (SoC, systemonchip) наблюдается процесс децентрализации обработки информации нижнего системного уровня [1], в конечной ситуации заключающийся в том, что в отдельные манипуляторы, датчики, исполнительные устройства встраивается собственная микропроцессорная система управления (МСУ) [2].

Таким образом, комплекс факторов определяет постоянное усложнение встраиваемых микропроцессорных систем. Отмечается быстрое внедрение принципов объектно-ориентированного программирования в разработку встраиваемого программного обеспечения и в АСУ ТП, что определяет гиперэкспоненциальный рост внутренней сложности, прежде всего, программных средств встраиваемых систем.

Особенность рассматриваемых программно-аппаратных встраиваемых систем состоит в том, что программное обеспечение (ПО) имеет большой объем, тесно связано с аппаратной частью и работает с периферией непосредственно.

В этой области существует определенная несогласованность мнений ведущих экспертов и документов в части определений компонент надежности, таких как функциональная[1] [3, 4], структурная [5], эксплуатационная, программная и аппаратная надежность.

Цель работы – разработка методики оценки функциональной надежности компонентов программно-аппаратной встраиваемой микропроцессорной системы управления и практическая оценка надежности актуальных на сегодняшний день программно-аппаратных компонент уровня встраиваемого компьютера и микроконтроллера для выбора оптимальной структуры системы управления.

1. Анализ состояния терминологии в области надежности встраиваемых систем

Вопросы, связанные с терминологией в области надежности, ставятся постоянно [6, 7], в том числе о терминологии надежности в области программного обеспечения [8]. Это объяснялось необходимостью обновления основного стандарта «Надежность в технике», определяющего терминологию в данной области, и необходимостью согласования основных используемых терминов с международными стандартами. Данный стандарт был обновлен, однако он не снял ряд вопросов.

Проблемы в основном возникают у специалистов, изучающих вопросы надежности информационных систем (ИС) в части их программной компоненты.

Стоит отметить определения д.т.н., профессора, официального эксперта Научного совета по информационной безопасности Совета Безопасности РФ Шубинского И.Б.: «функциональная надежность информационных систем в значительной мере зависит от надежности программных средств. Все принципы и методы обеспечения функциональной надежности программ, в соответствии с их целью, можно разделить на четыре группы: предупреждение ошибок, обнаружение ошибок, исправление ошибок и обеспечение устойчивости к ошибкам» [9]. Таким образом, надежность программных средств определяется как основа функциональной надежности.

Также следует выделить подробный анализ определения и содержания понятия объекта в надежности, выполненный д.т.н., профессором Нетесом В.А. В частности, было предложено уточнение понятия «объект»[2] как предмет рассмотрения, который наряду с аппаратными средствами может включать в себя программное обеспечение, необходимое для его функционирования [10].

В то же время, в ситуации программно-аппаратных комплексов степень взаимного влияния их составляющих – программного, аппаратного обеспечения, коммуникационных каналов – становится настолько сильной, что на показатели надежности программных средств влияет, в том числе, недекларированное поведение подсистем передачи данных и подсистем защиты от информационно-технических воздействий нарушителя (ИТВ).

Таким образом, формально функциональная надежность может быть снижена за счет частичного отказа компонент системы и т. д. В то же время информационная система в целом будет укладываться в требования технического задания по обеспечению основных своих функциональных характеристик за счет активных процессов восстановления, выполняемых встраиваемым программным обеспечением в автоматическом режиме.

Учитывая сложность определения и расчета параметров функциональной надежности гетерогенных информационных встраиваемых систем, на основе работ Шубинского И.Б., Нетеса В.А. и др., становится целесообразным определение понятия «информационная надежность» для встраиваемых программно-аппаратных микропроцессорных систем, часто относимых и к распределенным системам, которое характеризует степень соответствия основных показателей надежности системы тем, которые заложены в техническом задании или технических требованиях к гетерогенной информационной встраиваемой системе.

[1] ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.

[2] ГОСТ 27.002 2015 – устарел, взамен введен ГОСТ Р 27.102-2021 Надежность в технике. Надежность объекта. Термины и определения.

2. Методика оценки функциональной надежности компонент программно-аппаратной встраиваемой микропроцессорной системы управления

Методика оценки функциональной надежности компонент включает в свой состав четыре основных этапа, от анализа угроз компьютерных атак на компоненты до интерпретации результатов оценки надежности компонент встраиваемой программно-аппаратной системы.

1. Разработка модели функционирования микропроцессорной системы управления. Оценка рисков успешных ИТВ может выполняться на стендовом полигоне, позволяющем создать требуемые тестовые условия для работы функциональных аналогов МСУ, элементов СОПКА и имитации ИТВ.

Модель функционирования МСУ в условиях ИТВ, которая позволяет проводить комплексный анализ взаимосвязанных процессов функционирования МСУ, реализации ИТВ и ликвидации их последствий, в терминах расширенной сети Петри представлена в [11]. В разработанной модели предполагается, что МСУ оснащена коммуникационной подсистемой. Коммуникационная подсистема выполняет такие функции, как взаимодействие с промышленными системами более высокого уровня, удаленное считывание данных с датчиков и запись их значений в исполнительные устройства посредством сетевых интерфейсов.

В тоже время, для изолированной МСУ на первое место выходят требования к собственной функциональной надежности без учета внешних воздействий.

2. Показатели оценки функциональной надежности компонентов программно-аппаратной встраиваемой МСУ. Показатели оценки функциональной надежности МСУ могут определяться:

- эмпирически, на основе структурно-параметрического анализа особенностей построения, динамики функционирования и уязвимостей МСУ;

- экспериментально, на основании частоты успешно реализованных угроз ИТВ нарушителя, а также экспериментально на основе обработки большого массива данных по отказам аппаратных и программных средств. Подобный метод доступен производителям оборудования, результаты таких оценок доступны для некоторых аппаратных компонент. Установленные показатели надежности экстраполируются на весь жизненный цикл МСУ посредством введения динамической поправки, основанной на функции риска с использованием распределения Вейбулла-Гнеденко[1], а также [12].

Вычисление вероятности сбоев при передаче данных между элементами функционирования возможно осуществлять согласно [13]:

- вычисление вероятности того, что произойдет w_{pj} реальных сбоев при передаче данных между элементами функционирования за время $t_{СПДj}$ в j-м потоке передаче данных:

$$P_{СПД}^{СБР}\left(w_{рj}\right)=\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{Р}/\Delta t_{СПД}} P_{СПДj}^{Р\, w_{pj}},$$

где $w_{рj}$ – число реальных сбоев в средствах передачи данных;

$t_{СПД}^{СБ}$ – время, за которое происходит сбой в средствах передачи данных;

$P_{СПД_j}^{Р}$ – вероятность возникновения реального сбоя в j-м средстве передачи данных;

$\Delta t_{СПД}$ – среднее время передачи данных между элементами объектов МСУ;

k – число средств передачи данных.

- вычисление вероятности того, что произойдет $w_{дj}$ дополнительных (искусственно организованных) сбоев при передаче данных между элементами объектов МСУ за время $t_{СПДj}$ в j-м потоке передачи данных:

$$P_{СПД}^{СБД}\left(w_{дj}\right)=\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{Д}/\Delta t_{СПД}} P_{СПДj}^{Д\, w_{дj}},$$

где $w_{дj}$ – число дополнительных сбоев в средствах передачи данных;

$P_{СПД_j}^{Д}$ – вероятность возникновения дополнительного сбоя в j-м средстве передачи данных.

Оценка вероятности успешной передачи данных между элементами объектов МСУ осуществляется с использованием приведенных выше выражений.

$$P_{УСПД}=\frac{1}{N_w}\sum_{j=1}^{N_w} U_{P_{УСПД}}\left(w_{рj}, w_{дj}\right)\frac{\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{Р}/\Delta t_{СПД}} P_{СПДj}^{Р\, w_{pj}}}{\prod_{j=1}^{k} e^{-t_{СПДj}^{СБ} P_{СПДj}^{Д}/\Delta t_{СПД}} P_{СПДj}^{Р\, w_{дj}}},$$

где N_w – количество инструментальных оценок на стендовом полигоне с реализацией векторов сбоев $w_{рj}$ и $w_{дj}$;

$U_{P_{УСПД}}\left(w_{рj}, w_{дj}\right)$ – индикаторная функция, принимающая значение 1, если событие соответствует показателю $P_{УСПД}$, и 0 в противном случае.

3. Подготовка исходных данных для выполнения оценки функциональной надежности программно-аппаратных компонент МСУ. Исходные данные для эмпирической оценки собственной функциональной надежности программно-аппаратных компонент МСУ могут быть получены из ряда источников, таких как:

- данные Интернет-ресурсов, специализирующихся на анализе надежности аппаратных и программных средств;

- данные производителей, приводящих значения типовых показателей, таких как: MTTF (Mean Time to Failure); MTBF (Mean Time Between Failures); чаще для программного обеспечения может приводиться MTTD (Mean Time to Detection); MTTR (Mean Time to Recovery).

Несмотря на то, что для сложных программных систем, которые опираются на комплексное ПО, нет единого стандарта прогнозирования отказов [14], существует ряд методов, позволяющих получить приблизительные оценки отказов и, как следствие – надежности.

[1] ГОСТ Р 50779.27-2017 «Статистические методы. Распределение Вейбулла. Анализ данных»

Таким образом, используя один из методов, основанный на зависимости статистических показателей интенсивности отказов от объема ПО с применением модели Джелинского-Моранды [15], можно оценить интенсивность отказов программного комплекса $\lambda_{ПО}$

$$\lambda_{ПО} = \lambda \cdot K_р \cdot K_к \cdot K_з \cdot K_и,$$

где λ – интенсивность отказов разработанного ПО;

$K_р$ – коэффициент, отражающий влияние времени работы ПО;

$K_к$ – коэффициент, отражающий качество разработанного ПО;

$K_з$ – коэффициент, отражающий ремонтопригодность и частоту модернизаций разработанного ПО;

$K_и$ – коэффициент, отражающий загруженность и пользовательские изменения разработанного ПО.

В общем виде зависимость интенсивности отказов от объема ПО приведена в табл. 1.

Табл. 1. Зависимость интенсивности отказов от объема ПО

Тип управляющего ПО	Размер процессора	Объем ПО, Мб	$\lambda \cdot 10^{-6}$ $ч^{-1}$
Элементарная управляющая программа	С	0,25-1	0,4
Базовая управляющая программа	С	1,4-4,0	1,5
Расширенная управляющая программа	С	4,0-16	6
Базовая операционная система	С	16-64	25
Расширенная ОС	С	64-256	100
Управляющая программа	М	4-16	25
ОС с малыми возможностями	М/С	16-64	25
Универсальная ОС	С/Б	256+	100

4. Интерпретация результатов оценки компонентов программно-аппаратной встроенной МСУ. При анализе функциональной надежности в условиях ИТВ формой экспериментальной оценки может быть вычислительный эксперимент, проведенный с использованием стендового полигона, позволяющего создать требуемые тестовые условия для работы функциональных аналогов МСУ, элементов СОПКА и имитации ИТВ.

В случае анализа функциональной надежности программно-аппаратных компонент изолированной МСУ анализ функциональной надежности без учета факторов ИТВ целесообразно проводить на основании эмпирических данных. При этом в обязательном порядке требуется как оценка надежности аппаратной части с учетом структурной схемы соединения блоков, так и оценка надежности программного обеспечения.

Ниже приводится пример реализации представленной методики, которая включает в себя расчет основных компонент функциональной надежности – аппаратной и программной, для реальной гетерогенной по составу уровней встраиваемой системы управления на распространенном одноплатном компьютере RaspberryPi и компоненте нижнего системного уровня на микроконтроллере ATMega32. Ввиду отсутствия подсистем виртуализации в данной реализации нижнего системного уровня, имеются предпосылки к тому, чтобы она обладала более высоким уровнем надежности [9, 16].

Приведенная микропроцессорная система управления разрабатывается как система управления специализированным медицинским роботом, выполняющим функции удержания хирургических инструментов, ранорасширителей по Фараберу и пр. В состав системы входят следующие компоненты: микропроцессорный блок на распространенном одноплатном компьютере, реализующий высокоуровневые функции управления и распознавания голосовых команд, дополнительный микропроцессорный блок для управления сервоприводами и получения входных сигналов, а также исполнительные модули – приводы.

1) Разработка модели функционирования микропроцессорной системы управления. С учетом документа[1], формализация информационных процессов в микропроцессорной системе управления медицинским роботом в виде последовательной схемы показана на рис. 1.

[1] ГОСТ Р МЭК 61078-2021 Надежность в технике. Структурная схема надежности

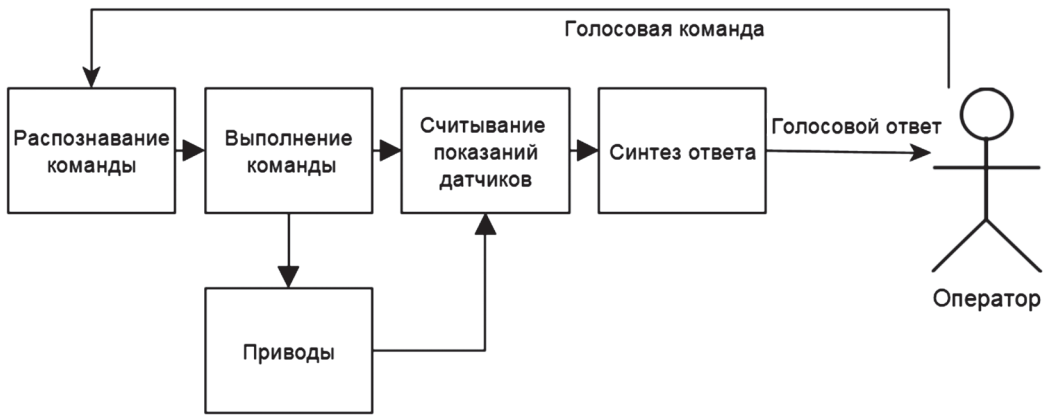


Рис. 1. Последовательная структура встраиваемой микропроцессорной системы управления медицинским роботом

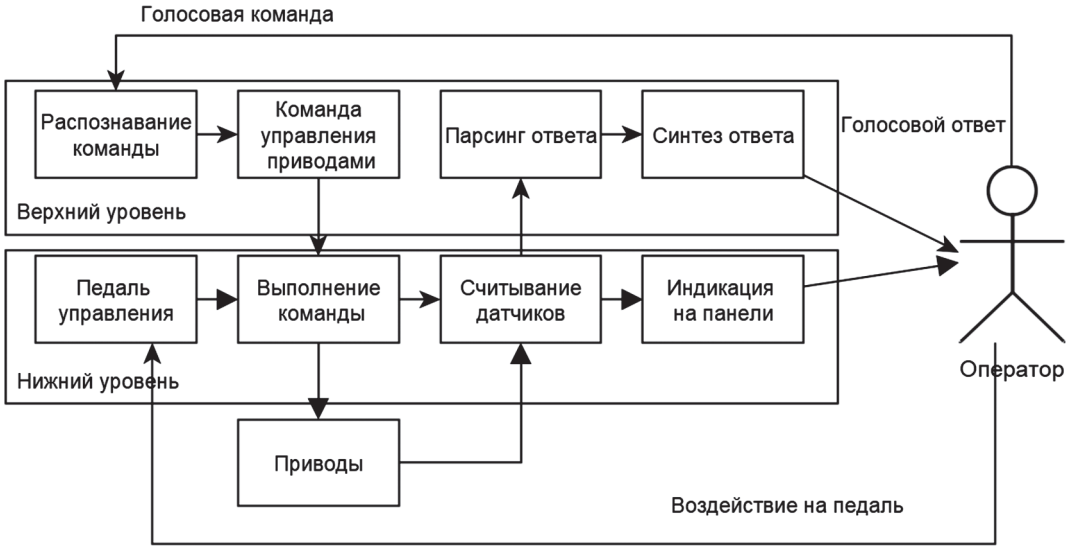


Рисунок 2. Структура системы с двумя уровнями

При такой структуре надежность всей системы является произведением компонент надежности $P_{ПО} = \prod_i P_{БЛi}$, где $P_{ПО}$ – вероятность безотказной работы программной системы в течение заданного времени, $P_{БЛi}$ – вероятность безотказной работы каждого (i-го) блока при аналогичных условиях.

Также необходимо учесть, что работоспособность всей системы зависит от работоспособности аппаратной части системы, поэтому $P_{СИСТ} = P_{ПО} \cdot P_{АО}$, где $P_{СИСТ}$ – вероятность безотказной работы системы, $P_{АО}$ – вероятность безотказной работы аппаратной части.

Альтернативная структурная схема МСУ с двумя уровнями, реализованная с использованием дополнительного модуля на микроконтроллере ATMega32 показана на рис. 2.

В качестве аппаратного обеспечения для расчетов выбран одноплатный компьютер RaspberryPi 4B.

2) Показатели оценки функциональной надежности компонентов программно-аппаратной встраиваемой МСУ. В данной работе в качестве показателя функциональной надежности программно-аппаратных компонент МСУ принимается вероятность безотказной работы в течение заданного промежутка времени.

3) Подготовка исходных данных для выполнения оценки функциональной надежности программно-аппаратных компонент МСУ. Из данных по надежности выбранного одноплатного компьютера Raspberry Pi 4B[1] известно, что среднее время между сбоями (*MTBF*) равно 27 тысяч часов, а интенсивность отказов λ равна $37 \cdot 10^{-6}$ч$^{-1}$. По данным сборника документов[2], интенсивность отказов выбранных исполнительных устройств можно оценить как $\lambda = 1{,}3 \cdot 10^{-6}$ ч$^{-1}$.

Вероятность безотказной работы аппаратной части в течение заданного промежутка времени вычисляется на основе экспоненциальной модели надежности, тогда для времени работы системы 12 ч вероятность безотказной работы одноплатного компьютера равна 0,9995, а вероятность безотказной работы приводов, используемых для фиксации подвижных элементов робота – 0,9999.

Используя метод, основанный на зависимости статистических показателей интенсивности отказов от объема ПО с применением модели Джелинского-Моранды, интенсивность отказов операционной системы одноплатного компьютера оценивается как $\lambda_{ОС} = 100 \cdot 10^{-6} \cdot 0{,}5 \cdot 0{,}5 \cdot 1 \cdot 2 = 50 \cdot 10^{-6}$ ч$^{-1}$, а интенсивность отказов модулей ПО $\lambda_{мод} = 25 \cdot 10^{-6} \cdot 2 \cdot 2 \cdot 0{,}5 \cdot 2 = 100 \cdot 10^{-6}$ ч$^{-1}$. Также, в качестве метода оценки надежности ПО возможно использовать количественную оценку, основанную на объеме ПО и типе языка программирования. Итоговые значения вероятности безотказной работы модулей системы управления с оценкой по статистическим показателям и по объему кода для операционной системы ($P_{ОС}$), программных модулей ($P_{мод}$) и всей системы ($P_{СИСТ}$), приведены в табл. 2.

Табл. 2. Оценка вероятности безотказной работы при заданных условиях

Параметр	Оценка по статистическим показателям	Оценка по объему кода
$P_{ОС}$	0,9994	0,9990
$P_{мод}$	0,9988	0,9994
$P_{СИСТ}$	0,9952	0,9966

В качестве альтернативы был выполнен расчет вероятности безотказной работы программных средств для структуры, когда часть важных функций разделена с дополнительным программно-аппаратным блоком, имеющим более высокий уровень надежности. В данном случае таким блоком является микроконтроллер (МК) Atmega32, который будет обеспечивать непо-

[1] По данным электронного ресурса Reliability

[2] Интенсивность отказов элементов справочник URL: https://areliability.com/intensivnost-otkazov-elementov-spravochnik

Табл. 3. Оценки вероятности безотказной работы

Вероятность безотказной работы	Одноуровневая система		Двухуровневая система	
	Оценка по статистическим показателям	Оценка по объему кода	Оценка по статистическим показателям	Оценка по объему кода
P_{RPi}	0,9995			
$P_{ОС}$	0,9994	0,9990	0,9994	0,9990
$P_{мод}$	0,9988	0,9994	0,9994	0,9990
$P_{МК}$	-	-	0,999999	
$P_{МК\_мод}$	-	-	0,999997	0,999999
$P_{СИСТ}$	0,9952	0,9966	0,9999999	0,9999999

средственное управление работой приводов. Для расчета аппаратной надежности МК доступны официальные отчеты фирмы-производителя, например, значение[1] среднего времени работы до наступления отказа *MTTF* = 186 655 346 ч. Альтернативный двухуровневый вариант структуры системы управления приведен в п. *1)* реализации методики и показан на рис. 2.

4) Интерпретация результатов оценки безотказной работы компонентов программно-аппаратной встроенной МСУ. Итоговые оценки вероятности безотказной работы модулей в заданных условиях для варианта с двумя уровнями и параллельным соединением блоков в сравнении с одноуровневой последовательной системой приведены в табл. 3.

При этом использованы следующие обозначения вероятностей безотказной работы при заданных условиях: P_{RPi} – для аппаратного обеспечения RaspberryPi 4B, $P_{ОС}$ – для программного обеспечения (встраиваемой операционной системы Linux), $P_{мод}$ – для программных модулей, $P_{МК}$ – для аппаратной части микроконтроллера, $P_{МК\_мод}$ – для программной части модулей ПО микроконтроллера, $P_{СИСТ}$ – итоговая вероятность безотказной работы всей системы при заданных условиях.

3. Обсуждение результатов

Как видно из табл. 2, в любом варианте оценки вероятность безотказной работы для достаточно малого интервала времени – 12 часов, является недостаточной. Важно отметить, что вероятность безотказной работы аппаратной части в течение заданного промежутка времени оценивается существенно выше, чем аналогичные показатели для программной части.

Как видно из табл. 3, за счет внедрения дополнительного уровня с частичным распараллеливанием функций и частичным резервированием каналов управления и индикации была значительно повышена оценка вероятности безотказной работы в заданных условиях системы, выполненной на актуальных на сегодняшний день программно-аппаратных устройствах.

[1] Reliability report microchip.com [Электронный ресурс] URL: https://www.microchip.com/reliabilityreport/#/

4. Выводы

Несмотря на тенденцию к интеграции максимального числа функций в единую систему на кристалле или в рамках одноплатного компьютера, для повышения вероятности безотказной работы встраиваемых программно-аппаратных микропроцессорных систем целесообразным является их двухуровневое построение, при котором ключевые задачи в части непосредственной работы с аппаратным окружением перераспределяются в пользу отдельного аппаратного модуля. Такой модуль должен строиться на микроконтроллере, а его программное обеспечение – иметь самый низкий из возможных уровней виртуализации или не иметь его вовсе. Кроме того, данный модуль может также выполнять функции аппаратного гипервизора, контролируя работоспособность верхнего аппаратного уровня и, при необходимости, выполнять его перезагрузку, не прерывая выполнения собственных задач.

С использованием указанного подхода была построена система управления медицинским роботом, и проведенное всестороннее тестирование не выявило отказов или сбоев в работе.

В то же время при анализе методов оценки надежности программно-аппаратных встраиваемых систем было установлено, что практические методы испытаний на отказ подразумевают множественное повторение условий экспериментов и воздействий, и на этом основании строится вероятностная оценка. К тому же, как показано в работе, надежность базового аппаратного обеспечения достаточно высока и значение вероятности программного отказа может быть существенно выше, чем аппаратного. Для встраиваемых систем нижнего уровня, в котором программная компонента непосредственно связана с аппаратной частью, периферией и цифровыми интерфейсами, методы практической оценки вероятности отказа было бы целесообразно дорабатывать с учетом особенностей рассматриваемых систем.

Библиографический список

1. Deepa V.V., Thamotharan B., Mahto D. et al. Smart embedded health monitoring system and secure electronic health record (EHR) transactions using blockchain

technology // SoftComput. 2023. Vol. 27. Pp. 12741–12756. DOI: 10.1007/s00500-023-08893-4

2. Siraj I., Bharti P.S. Reliability analysis of a 3D Printing process // Procedia Computer Science. 2020. Vol. 173. Pp. 191-200. DOI: 10.1016/j.procs.2020.06.023

3. Shubinsky I.B., Schäbe H. On the definition of functional reliability // RT&A. 2012. № 4(27). URL: https://cyberleninka.ru/article/n/on-the-definition-of-functional-reliability (дата обращения: 12.08.2024).

4. Burgazzi L. Reliability Evaluation of Passive Systems Through Functional Reliability Assessment // NuclearTechnology. 2003. Vol. 144. DOI: 10.13182/NT144-145.

5. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.

6. Ершов Г.А., Семериков В.Н., Семериков Н.В. Чему верить? О системе стандартов «Надежность в технике» // Стандарты и качество. 2018. № 8. С. 14-19.

7. Нетес В.А. Как вернуть доверие? О системе стандартов «Надежность в технике» // Стандарты и качество. 2019. № 2. С. 19-24.

8. Потапов И.В., Баева М.А. Вопросы терминологии надежности в области программ и программных средств // Надежность. 2015. № 4. С. 65-74. DOI: 10.21683/1729-2646-2015-0-4-65-74

9. Шубинский И.Б. Методы обеспечения функциональной надежности программ // Надежность. 2014. № 4. С. 87-101. DOI: 10.21683/1729-2646-2014-0-4-87-101

10. Нетес В.А. Объект в надежности: определение и содержание понятия // Надежность. 2019. № 19(4). С. 3-7. DOI: 10.21683/1729-2646-2019-19-4-3-7

11. Климов С.М., Сосновский Ю.В. Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий // Надежность. 2018. № 18(4). С. 36-44. DOI: 10.21683/1729-2646-2018-18-4-36-44

12. Капур К., Ламберсон Л. Надежность и проектирование систем / под ред. И.А. Ушакова. Пер. с англ. М.: «Мир», 1980. 604 с., ил.

13. Системное обоснование концептуальных положений применения передовых космических технологий / под ред. В.М. Буренка и А.Е. Тюлина. М.: Инновационное машиностроение, 2023. 372 с., ил.

14. Littlewood B., Strigini L. Validation of Ultra-High Dependability for Software-based Systems // Commun. ACM. 1993. Vol. 36. Pp. 69-80. DOI: 10.1145/163359.163373

15. Предложение по определению эксплуатационной надежности программного обеспечения сложных технических систем / А.С. Белов, М.М. Добрышин, А.Н. Горшков, Д.Е. Шугуров // Известия Тульского государственного университета. Технические науки. 2022. № 9. С. 143-148. DOI: 10.24412/2071-6168-2022-9-143-148

16. Ивутин А.Н., Суслин А.А. О некоторых применениях статистических распределений в оценке надежности программного обеспечения // Известия ТулГУ. Технические науки. 2011. № 2. С. 568-575.

References

1. Deepa V.V., Thamotharan B., Mahto D. et al. Smart embedded health monitoring system and secure electronic health record (EHR) transactions using blockchain technology. *SoftComput* 2023;27:12741–12756. DOI: 10.1007/s00500-023-08893-4.

2. Siraj I., Bharti P.S. Reliability analysis of a 3D Printing process. *Procedia Computer Science* 2020;173:191-200. DOI: 10.1016/j.procs.2020.06.023.

3. Shubinsky I.B., Schäbe H. On the definition of functional reliability. *RT&A* 2012;4(27). (accessed 12.08.2024). Available at: https://cyberleninka.ru/article/n/on-the-definition-of-functional-reliability.

4. Burgazzi L. Reliability Evaluation of Passive Systems Through Functional Reliability Assessment. *Nuclear Technology* 2003;144. DOI: 10.13182/NT144-145.

5. Shubinsky I.B. [Structural dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012. (in Russ.)

6. Yershov G.A., Semerikov V.N., Semerikov N.V. [What to believe? On the system of standards “Dependability in engineering”]. *Standarty i kachestvo* 2018;8:14-19. (in Russ.)

7. Netes V.A. [How to regain trust? About the system of standards “Dependability in engineering”]. *Standarty i kachestvo* 2019;2:19-24. (in Russ.)

8. Potapov I.V., Baeva M.A. Terminology issues related to reliability of programs and software. *Dependability* 2015;(4):65-74. DOI: 10.21683/1729-2646-2015-0-4-65-74.

9. Shubinsky I.B. Methods of software functional dependability assurance. *Dependability* 2014;(4):87-101. DOI: 10.21683/1729-2646-2014-0-4-87-101.

10. Netes V.A. Item in dependability: definition and content of the concept. *Dependability* 2019;19(4):3-7. DOI: 10.21683/1729-2646-2019-19-4-3-7.

11. Klimov S.M., Sosnovsky Yu.V. Method of assessing the protection of computer-based control systems under information technology interference. *Dependability* 2018; 18(4):36-44. DOI: 10.21683/ 1729- 1729-2646-2018-18-4- 44.

12. Kapur K., Lamberson L. Ushakov I.A., editor. Reliability in Engineering Design. Moscow: Mir; 1980.

13. Burenok V.M., Tyulin A.E., editors. [Systematic substantiation of the conceptual provisions of the application of advanced space technologies]. Moscow: Innovatsionnoye mashinostroyeniye; 2023. (in Russ.)

14. Littlewood B., Strigini L. Validation of Ultra-High Dependability for Software-based Systems. *Commun. ACM* 1993;36:69-80. DOI: 10.1145/163359.163373.

15. Belov A.S., Dobrynin M.M., Gorshkov A.A., Shugurov D.E. Proposal for determining the operational reliability of software complex technical systems. *News of*

the Tula state university. Technical sciences 2022;9:143-148. DOI: 10.24412/2071-6168-2022-9-143-148. (in Russ.)

16. Ivutin A.N., Suslin A.A. Some remarkable appliances of statistical distributions in software reliability estimation. *News of the Tula state university. Technical sciences* 2011;2:568-575. (in Russ.)

Сведения об авторах

Сергей М. Климов – доктор технических наук, профессор МГТУ им. М.Э. Баумана, профессор, e-mail: klimov.serg2012@yandex.ru.

Юрий В. Сосновский – кандидат технических наук, доцент кафедры компьютерной инженерии и моделирования Физико-технического института Крымского федерального университета им. В.И. Вернадского, e-mail: yuri.sosnovskij@yandex.ru

Денис Р. Чачиев – магистр, специалист кафедры компьютерной инженерии и моделирования Физико-технического института Крымского федерального университета им. В.И. Вернадского, e-mail: denis.chachiev@mail.ru.

About the authors

Sergey M. Klimov, Doctor of Engineering, Professor, Bauman Moscow State Technical University, Professor, e-mail: klimov.serg2012@yandex.ru.

Yuri V. Sosnovsky, Candidate of Engineering, Senior Lecturer, Department of Computer Engineering and Modeling, Physics and Technology Institute, Crimean Federal University named after V.I. Vernadsky, e-mail: yuri.sosnovskij@yandex.ru.

Denis R. Chachiev, Master Student, Specialist, Department of Computer Engineering and Modeling, Physics and Technology Institute, Crimean Federal University named after V.I. Vernadsky, e-mail: denis.chachiev@mail.ru.

Вклад авторов в статью

Автором **Климовым С.М.** выполнена постановка задачи разработки встраиваемой программно-аппаратной системы управления медицинского робота и необходимость оценки компонент программной и аппаратной надежности системы. Разработаны методы вычисления вероятности сбоев при передаче данных между элементами функционирования информационной системы.

Автором **Сосновским Ю.В.** выполнен анализ литературы по теме исследования, определены понятия «функциональная надежность» и «информационная надежность» для встраиваемых программно-аппаратных микропроцессорных систем, часто относимых и к распределенным системам. Функциональная надежность характеризует степень соответствия основных показателей надежности системы тем, которые заложены в техническом задании или технических требованиях к функциональным возможностям гетерогенной информационной встраиваемой системы.

Автором **Чачиевым Д.Р.** был выполнен анализ регламентирующих документов и источников в Интернет, рассчитаны значения вероятности безотказной работы компонент системы в течение выбранного промежутка времени – 12 часов, разработана структурная схема встраиваемой микропроцессорной системы управления двух альтернативных вариантов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.