УДК 621.316.925.1
DOI: 10.53015/18159958_2025_21_2_38

РАЗРАБОТКА ТЕРМИНАЛА МИКРОПРОЦЕССОРНОЙ РЕЛЕЙНОЙ ЗАЩИТЫ С ПОВЫШЕННОЙ НАДЕЖНОСТЬЮ И ЭФФЕКТИВНЫМИ ЭКОНОМИЧЕСКИМИ ПОКАЗАТЕЛЯМИ

DEVELOPMENT OF A MICROPROCESSOR RELAY PROTECTION TERMINAL WITH INCREASED RELIABILITY AND EFFICIENT ECONOMIC PERFORMANCE

©2025
Паринов Максим Викторович, кандидат технических наук, доцент кафедры механотроники и робототехники
Горемыкин Сергей Александрович[1], кандидат технических наук, доцент кафедры электромеханических систем и электроснабжения
Ситников Николай Васильевич[2], кандидат технических наук, доцент кафедры электромеханических систем и электроснабжения
Шелякин Валерий Петрович, кандидат технических наук, доцент кафедры электромеханических систем и электроснабжения

Parinov Maxim Viktorovich, Candidate of Technical Sciences, Associate Professor of the Department of Mechanotronics and Robotics
Goremykin Sergey Alexandrovich[1], Candidate of Technical Sciences, Associate Professor of the Department of Electromechanical Systems and Power Supply
Sitnikov Nikolay Vasilyevich[2], Candidate of Technical Sciences, Associate Professor of the Department of Electromechanical Systems and Power Supply
Shelyakin Valery Petrovich, Candidate of Technical Sciences, Associate Professor of the Department of Electromechanical Systems and Power Supply

Воронежский государственный технический университет, Воронеж (Россия)
Voronezh State Technical University, Voronezh (Russia)

E-mail: parmax@mail.ru
E-mail: goremykinsa@yandex.ru [2]ORCID: https://orcid.org/0000-0002-1911-4986
E-mail: nvs17939@mail.ru [3]ORCID: https://orcid.org/0000-0002-0179-1372
E-mail: 437712@mail.ru

Аннотация: В статье предлагается концепция создания микропроцессорного терминала релейной защиты, обладающего повышенной надежностью и невысокой стоимостью. Результат достигается применением мажоритарной схемы управления, специального программного обеспечения, современной элементной базы и оптимизации функциональности. Программное обеспечение использует многопоточность и взаимодействует с операционными системами реального времени. Это обеспечивает повышение надежности как посредством распределения процессов между модулями мажоритарной схемы управления, так и с помощью многопоточных инкапсулированных вычислений при работе каждого отдельного ядра терминала.

Ключевые слова: релейная защита, микропроцессорный терминал, быстродействие, функциональность, надежность, имитационное моделирование, многопоточная схема, мажоритарная схема управления.

Для цитирования: Разработка терминала микропроцессорной релейной защиты с повышенной надежностью и эффективными экономическими показателями / М.В. Паринов, С.А. Горемыкин, Н.В. Ситников, В.П. Шелякин // Вести высших учебных заведений Черноземья. – 2025. – Т. 21, № 2 (78). – С. 38-47. – DOI 10.53015/18159958_2025_21_2_38.

Abstract: The article proposes a concept for creating a microprocessor-based relay protection terminal with increased reliability and low cost. The result is achieved by using a majority control scheme, special software, a modern element base and optimization of functionality. The software uses multithreading and interacts with real-time operating systems. This provides increased reliability both through the distribution of processes between the modules of the majority control system, and through multithreaded encapsulated computing during the operation of each individual terminal core.

Keywords: relay protection, microprocessor terminal, performance, functionality, reliability, simulation, multithreaded circuit, majority control circuit.

For citation: Development of a microprocessor relay protection terminal with increased reliability and efficient economic performance / M.V. Parinov, S.A. Goremykin, N.V. Sitnikov, V.P. Shelyakin // Vesti of Higher Educational Institutions of the Chernozem region. – 2025. – Vol. 21, № 2 (78). – P. 38-47. – DOI 18159958_2025_21_2_38.

ВВЕДЕНИЕ

Необходимость применения устройств релейной защиты не подлежит обсуждению. Однако методы ее реализации значительно варьируются. В настоящее время в развитых странах подавляющее большинство устройств релейной защиты относится к микропроцессорным устройствам высокой степени интеграции. Однако значительная часть современных решений реализуется на упрощенной элементной базе, в том числе на электромагнитных реле. Основная причина отказа от современных микропроцессорных терминалов – значительная разница в стоимости оборудования. Обычно она является обоснованной. Однако существует ряд других причин, не являющихся однозначными.

Например, в работах [1–3] авторы утверждают, что надежность сложных микропроцессорных терминалов защиты уступает данному параметру у классических релейных решений. Также ими отмечена сложность и дороговизна обслуживания подобных устройств. Однако данному мнению чаще противопоставляются другие исследования [4, 5, 18]. Несмотря на значительное количество материалов на данную тему, точный ответ на вопрос получить практически невозможно, так как для этого требуется обширный анализ данных об эксплуатации устройств, принадлежащих коммерческим организациям.

Анализ доводов авторов источников [1–5] позволяет определить особенности каждого из типов защиты, отрицательно влияющие на эксплуатационные характеристики. Показатели надежности классических релейных схем в настоящее время хорошо изучены, а уровень развития данных технологий практически не позволяет их улучшить без значительного ухудшения экономических характеристик. При этом данные решения значительно уступают по быстродействию и функциональности. Если вопрос быстродействия на практике не является острым, так как классические релейные защиты обычно справляются с поставленной задачей, то функциональность однозначно объясняет преимущества микропроцессорных устройств релейной защиты.

Микропроцессорные защиты позволяют реализовать значительное (теоретически бесконечное) количество защитных функций в одном блоке. Значительное преимущество микропроцессорных устройств выражено возможностью реализации упреждающих аварийные ситуации функций [6]. Одним из механизмов упреждения и ранней локализации аварии является возможность применения алгоритмов искусственного ин-

теллекта [7], что абсолютно недопустимо для классических решений. Актуальность реализации централизованных систем управления и диспетчеризации также показывает преимущество микропроцессорных защит.

Однако неоднозначными являются показатели надежности, долговечности и сложности обслуживания микропроцессорных решений. На основании собственного опыта и анализа источников [1–5] нами были определены их следующие потенциальные недостатки:

1. Ошибки программного обеспечения микропроцессорных терминалов.
2. Ошибки эксплуатации вследствие несоответствия квалификации персонала.
3. Высокая сложность и стоимость обслуживания.
4. Малая долговечность.
5. Отсутствие аппаратных средств резервирования функциональных блоков.
6. Низкое качество аппаратной реализации устройств.

ИССЛЕДОВАНИЕ

Нами предлагается решение, которое позволяет не только значительно уменьшить перечисленные недостатки, но и снизить его стоимость, сделав ее соизмеримой с классическими релейными решениями, что важно для регионов с невысокими экономическими показателями. Для его реализации необходимо решить следующие задачи:

1. Определить минимальную достаточную функциональность.
2. Минимизировать аппаратное обеспечение посредством оптимизации конструкции и применения современной элементной базы.
3. Отказаться от использования элементов с ограниченной долговечностью и/или требующих обслуживания.
4. Создать достаточное резервирование аппаратного обеспечения микропроцессорного терминала защиты.
5. Разработать концепцию программного управления с повышенной надежностью, использующую механизмы резервирования, многопоточности и мажоритарного управления.

Определение минимальной и достаточной функциональности необходимо для корректной реализации задач 2–5. Вероятность возникновения ошибок системы складывается из соответствующих параметров для каждого функционального блока. Однако для современных аппаратно-программных решений линейное суммирование вероятностей не является корректным, так как при взаимодействии между функциональными блоками растет вероятность ошибок системы согласно их количеству, надежности и особенностям условий работы

$$P_{fg}=K^{\sum_{i=0}^{n} P_i K_{ip}}+ \sum_{i=0}^{n} P_i K_{im} \qquad (1)$$

Нашей задачей является минимизация вероятности полного отказа P_{fg}. При этом необходимым условием является сохранение заданной функциональности. Данный подход позволит, отказавшись от формальных функций, не только повысить стабильность, но и уменьшить стоимость защиты вследствие упрощения аппаратного и программного обеспечения.

Минимизация аппаратного обеспечения предполагает использование современных микроконтроллеров высокой степени интеграции. Это позволяет отказаться от значительного количества дополнительных элементов. В частности, в современные микроконтроллеры среднего и верхнего диапазона встроены все необходимые цифровые интерфейсы, а также АЦП с параметрами, превосходящими требования релейной защиты. Их использование позволяет без ущерба функциональности уменьшить до минимума число радиотехнических элементов блока, что обеспечит не только максимальную надежность, но и низкую стоимость. Стоимостные характеристики объясняются низкой ценой современных микроконтроллеров, малым количеством деталей и простотой изготовления электронного блока.

На рис. 1 показана классическая схема реализации терминала микропроцессорной защиты. В верхнем ряду справа находится микропроцессорный модуль. Слева от него блок аналого-цифрового преобразования. Данные блоки в современных условиях успешно заменяются электроникой, пока-

занной на рис. 2. Также она может частично выполнять функции модуля пользовательского интерфейса и дискретных интерфейсов, которые показаны в нижнем ряду на рис. 1.

Необходимым решением для значительного повышения надежности и долговечности является отказ от классических электролитических конденсаторов. Данный тип элементов практически единственный тип деталей, который ограничивает долговечность и требует планового ремонта электронной техники. Высокие эксплуатационные характеристики также достигаются предварительным имитационным моделированием платы с дальнейшим натурным экспериментом в максимально сложных рабочих условиях. Все характеристики электронных компонентов должны быть выбраны с запасом [8].

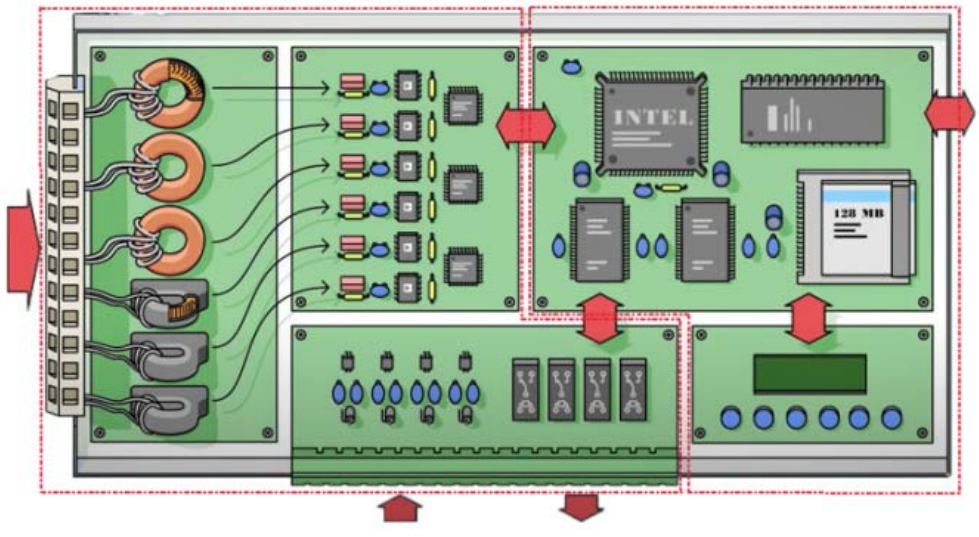


Рис. 1. Классическая схема реализации терминала микропроцессорной релейной защиты
Fig. 1. Classical scheme of implementation of the microprocessor relay protection terminal

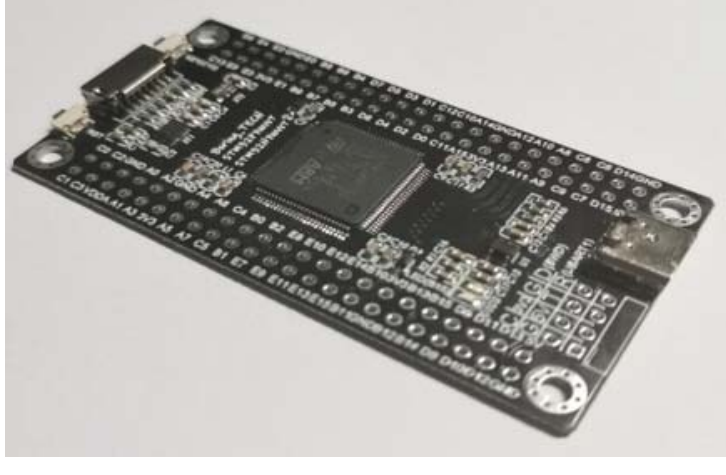


Рис. 2. Главный модуль терминала микропроцессорной релейной защиты
Fig. 2. Main module of the microprocessor relay protection terminal

Данный подход практически не влияет на итоговую стоимость изделия, но значительно повышает его надежность.

Вопрос резервирования аппаратной базы решается на основании выбора компромисса между надежностью и стоимостью изделия. Нами предлагается два варианта реализации. Упрощенное решение использует двойное резервирование цепей питания. Цепи анализа сигнала и управления не дублируются. Однако с целью повышения надежности предлагается использовать ряд типо-

вых решений, обеспечивающих автоматический контроль и исправление аварийных ситуаций посредством трёх независимых микроконтроллерных устройств.

Подобный подход доказал свою эффективность в устройствах с крайне высокими требованиями надежности [10, 11]. В связи с появлением недорогих многофункциональных быстродействующих микроконтроллеров, он может быть успешно применен в микропроцессорном терминале защиты. Нами предлагается три независимых микропроцессорных блока, каждый из которых имеет собственный модуль питания и входные цепи аналого-цифровых преобразователей. Между блоками реализовано два независимых интерфейса обмена данными (например, CAN и Ethernet). Все цепи питания, измеряемые сигналы и интерфейсы гальванически изолированы. В случае работы с потенциально опасным входным сигналом допускается реализация устройства в различных корпусах или в различных изолированных отсеках одного корпуса.

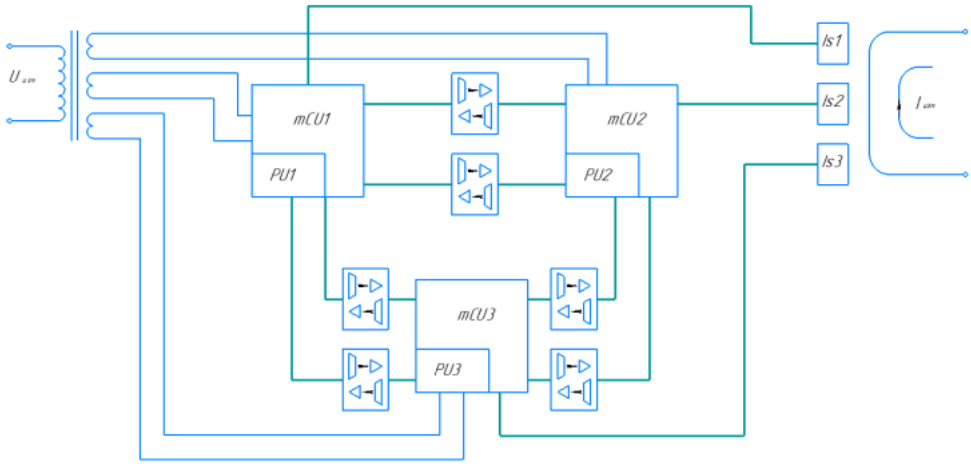


Рис. 3. Структурная схема аппаратной реализации устройства
Fig. 3. Block diagram of the hardware implementation of the device

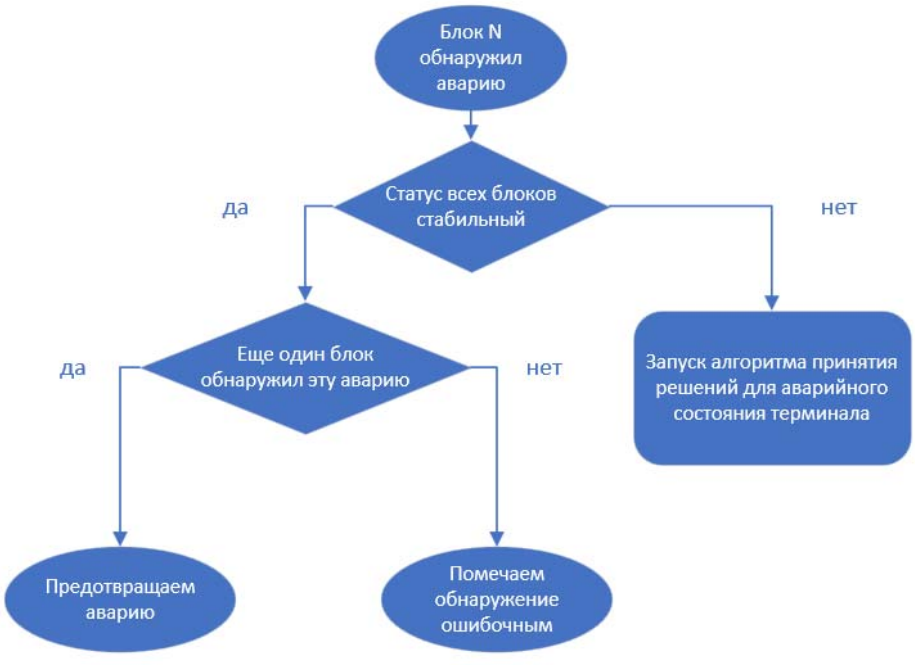


Рис. 4. Алгоритм реализации мажоритарной схемы управления
Fig. 4. Algorithm of implementation of the majority management scheme

Для распределенной системы в качестве максимально простых и надежных интерфейсов связи между микроконтроллерными блоками могут быть использованы интегрированные в микроконтроллер Bluetooth и WiFi.

На рис. 3 показана структурная схема предложенной концепции. Она показывает, что каждый из блоков реализует полностью независимый функционал релейной защиты.

Между блоками отсутствует гальваническая связь. Все блоки питания индивидуальные. Датчики индивидуальны, разделены трансформаторами или реализованы по бесконтактной схеме.

Интерфейсы обеспечивают связь между всеми блоками попарно. Каждая линия связи представлена двумя полностью независимыми интерфейсами. Гальваническая связь по линиям связи отсутствует. Разделение осуществляется с помощью типовых изолирующих буферов.

Программное обеспечение содержит ряд особенностей, обеспечивающих значительное повышение надежности по сравнению с классическими решениями. Одной из них является мажоритарное управление, базовый алгоритм которого показан на рис. 4.

Основная идея заключается в одновременной параллельной работе всех микропроцессорных модулей. При обнаружении аварии в контролируемой сети модуль опрашивает другие 2 модуля. Если хотя бы один из них имеет аналогичные данные, принимается решение о начале соответствующей данной аварии процедуры. Однако это условие выполняется, если регулярный опрос показывает, что статус всех блоков стабилен. Если в процессе работы установлено, что один из блоков не функционирует в соответствии с установленными требованиями, то при обнаружении аварии запускается алгоритм обработки события для аварийного состояния блока защиты.

Для подтверждения работоспособности микропроцессорных модулей и их интерфейсов с заданной частотой выполняется обмен контрольными данными. В случае обнаружения сбоев выполняется процесс перезапуска программных модулей, устройств или переключение информационных интерфейсов. Для этого нами разработан ряд алгоритмических и программных решений, описание которых выходит за рамки данной работы. Также применены широко известные методы программного управления с повышенной надежностью [12, 13, 22, 23].

Отдельно следует отметить подход многопоточного параллельного выполнения программного кода. Его пример показан на рис. 5, где каждый из программных обработчиков токовой защиты реализован в виде отдельного потока. Данный процесс вызывает некоторые разногласия при определении надежности.



Рис. 5. Реализация параллельных потоков
Fig. 5. Implementation of parallel streams

Например, источник [14] считает, что параллельное выполнение программы значительно повышает вероятность сбоев. Однако эти утверждения в источнике не обоснованы, а описание применяемых средств говорит о том, что авторы реализуют неординарную разработку или плохо владеют современными технологиями.

Нами предлагается использование многопоточности в качестве одного из основных механизмов повышения надежности. При использовании последовательного выполнения кода в одном потоке программы сбой любого из ее элементов с высокой вероятностью вызовет ее аварию. При этом страдают все функции программы. При многопоточном параллельном вычислении сбой одного из потоков при отсутствии прямого взаимодействия с другими потоками обычно не влияет на работоспособность остальных элементов программы. Исключением являются зависания на уровне ядра. Данный вид ошибок сравнительно редок и может быть значительно минимизирован применением программных диспетчеров.

Выражение

$$P_{fg_mult} = \max(P_1 \ldots . P_n) + \sum_{i=0}^{n} P_i K_{ik_mult} + P_{sc},$$

показывает, что при параллельной многопоточной схеме общая вероятность складывается из максимальной вероятности сбоя параллельных потоков, а также суммы вероятностей сбоя всех потоков, умноженной на малый коэффициент. Данная часть выражения описывает вероятность возникновения фатальных ошибок, влияющих на соседние потоки или останавливающих ядро. Его значение минимально по сравнению с другими слагаемыми. Третьим компонентом является вероятность сбоя диспетчера многопоточного приложения. Его значение невелико и зависит от применяемых технологий.

В качестве диспетчера может быть использована оригинальная разработка или операционная система реального времени [15, 16, 19]. Известно мнение, что применение операционных систем отрицательно влияет на надежность и время реагирования системы [16]. Однако нам неизвестны обоснованные доводы о снижении надежности. При этом известно значительное количество исследований, показывающих очень высокую надежность популярных операционных систем реального времени [15, 17].

Авторы согласны с незначительным ухудшением временных характеристик управления при использовании операционной системы. Однако при учете скорости процессов, которые контролирует блок релейной защиты, этими данными можно пренебречь. Поэтому с учетом отличных показателей надежности [17] и хорошей функциональности принято решение об использовании операционной системы FreeRTOS в качестве средства управления многопоточным программным обеспечением.

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ И ВЫВОДЫ

Рассмотренная в статье концепция построения терминала релейной защиты на данный момент находится в стадии разработки. В настоящее время нами реализованы блоки максимальной токовой защиты на микроконтроллере STM32f769 [20]. Программное обеспечение выполнено по многопоточной схеме под управлением операционной системы FreeRTOS. Программирование выполнялось с использованием моделей верхнего уровня (HAL) [21]. Данный подход теоретически опасен избыточностью функций, что с точки зрения абстрагированной от объекта математической оценки может уменьшить надежность устройства. Однако на практике типовое апробированное программное обеспечение практически всегда показывает лучшие показатели надежности, чем разработка собственных программных элементов.

Короткое тестирование (десятки – сотни тестов) показало, что после завершения отладки текущая версия предложенного решения абсолютно стабильна. Однако с учетом требований к рассматриваемому типу оборудования необходимо исследование, включающее миллионы и десятки миллионов тестов, что недостижимо в условиях университетской лаборатории. По этой причине в настоящее время нам не удалось определить практическую ценность мажоритарной схе-

мы управления разрабатываемого терминала защиты.

Однако опыт нашего коллектива разработки электрических и бортовых систем космических и летательных аппаратов подтвердил (в том числе практическими исследованиями) эффективность всех решений, предложенных в статье. До недавнего времени распределение данного подхода за пределы высокобюджетных сред было практически невозможным. Однако с появлением современных недорогих быстродействующих контроллеров это ограничение снято.

В настоящее время мы продолжаем работу над представленным терминалом релейной защиты. Планируется кооперация с производственными мощностями, что необходимо для выхода на рынок и выполнения полного цикла исследований.

ЗАКЛЮЧЕНИЕ

В рассмотренной статье предложен принципиально новый подход применения мажоритарной схемы управления на трех независимых микроконтроллерных устройствах, что позволяет многократно повысить надежность микропроцессорного терминала релейной защиты при минимизации стоимостных показателей данного устройства. Также следует отметить оригинальность реализации подхода параллельных потоков применительно к обработке сигналов токовых защит, что является одним из определяющих факторов повышения надежности устройства в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Гуревич В.И. Проблемы оценки надежности релейной защиты // Электричество. 2011. № 2. С. 28-31.

2. Гуревич В.И. Микропроцессорные реле защиты: в поисках оптимальности // Энергетика и промышленность России. 2009. № 21 (137), ноябрь.

3. Гуревич В.И. Новая концепция построения микропроцессорных устройств релейной защиты // Компоненты и технологии. 2010. № 6. С. 12-14.

4. Захаров О.Г. Манипулирование «вопросами» в релейной защите // Энергетика и ТЭК. 2010. № 2. С. 47.

5. Захаров, О.Г. Надежность цифровых устройств релейной защиты. Показатели. Требования. Оценки : практическое пособие. Москва : Инфра-Инженерия, 2014. 128 с. ISBN 978-5-9729-0073-2 ; Директ-Академия : сайт. URL: https://biblioclub.ru/index.php?page=book&id=234786 (дата обращения: 21.04.2021).

6. Булычев А., Нудельман Г. Релейная защита. Совершенствование за счет упреждающих функций // Новости электротехники. 2009. № 4 (58). С. 30-33.

7. Камель Т.С., Хассан М.А., Эль-Моршеди А. Применение систем искусственного интеллекта в дистанционной защите линии электропередачи // Тезисы докладов Второй Международной научно-технической конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Москва, 7-10 сентября 2009 г. Москва, 2009. С. 30-38.

8. К вопросу о проектировании и эксплуатации микропроцессорных устройств релейной защиты / А.В. Сычев Л.И. Евминов, В.В. Курганов, А.Н. Гуминский // Вестник ГГТУ имени П.О. Сухого : научно-практический журнал. 2009. № 4. С.73-79.

9. Бестемьянов П.Ф. Методы обеспечения безопасности аппаратных средств микропроцессорных систем управления движением поездов // Электротехника. 2020. № 9. С. 2-8.

10. Тильк И.Г., Ляной В.В., Абакумов М.В. Система микропроцессорной централизации МПЦ-И // ЖДМ. 2007. № 1. С. 63-66.

11. Синтез схемы управляемого мажоритарного элемента для резервированных систем управления / Р.С. Кулиев, С.Н. Сыцевич, Ж.Ж. Жабоев, И.И. Таукенов // Современные наукоемкие технологии. 2016. № 9-1. С. 63-66.

12. Ширяев М.И., Лавров К.Ю. Андреева О.Н. Совершенствование способа повышения надежности специального программного обеспечения встраиваемых систем // Нейрокомпьютеры: разработка, применение. 2014. № 5. С. 38-45.

13. Гассельберг В.С., Синельщиков А.В. Применение микроконтроллеров в устройствах с повышенной надежностью // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2011. № 1. С. 108-113.

14. Типикина А.П., Певцова Л.С. Оценка программной надежности микропроцессорных релейных защит. DOI 10.15862/74TVN215) // Интернет-журнал «Науковедение». 2015. Т. 7, № 2. http://naukovedenie.ru/PDF/74TVN215.pdf (доступ свободный). Загл. с экрана.

15. Щербаков К.С., Щербаков С.А. Особенности работы операционной системы реального времени FreeRTOS // Itech. Журнал интеллектуальных технологий. 2011. № 18. С. 71-77.

16. Гома Х. UML-проектирование систем реального времени параллельных и распределенных приложений // ДМК-Пресс, 2011. 704 с. ; National Instrument hat is a Real-Time Operating System (RTOS)? Режим доступа: http://www.ni.com/white-paper/3938/en/ (дата обращения: 24.12.2016.)

17. Назаров С.В., Барсуков А.Г. Архитектура и надежность операционных систем // Современные информационные технологии и ИТ-образование. 2018. № 1. С. 38-51. URL: http://elib.fa.ru/art2018/bv2476.pdf. (дптп обращения: 24.12.2016).

18. Zamani M.A., Sidhu T.S. Yazdani A. A protection strategy and microprocessor-based relay for low-voltage microgrids. DOI 10.1109/TPWRD.2011.2120628 // IEEE transactions on Power Delivery. 2011. № 26 (3). P. 1873-1883.

19. Hambarde P., Varma R., Jha S. The survey of real time operating system: RTOS // 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies. 2014. January. P. 34-39.

20. Brown G. Discovering the STM32 microcontroller. 2012. № 3 (34). P. 64.

21. Kröning M.W. Concurrency Techniques and Hardware Abstraction Layer Concepts for Embedded Systems in Rust : Doctoral dissertation. Universitätsbibliothek der RWTH. Aachen, 2023.

22. Pham H. System software reliability. Cham (ZG). Springer Science & Business Media, 2007. 454 p.

23. Laprie J.C., Kanoun K. Software reliability and system reliability // Handbook for Software Reliability Engineering. 1996. P. 27-69.

REFERENCES

1. Gurevich V.I. Problems of assessing the reliability of relay protection // Electricity. 2011. № 2. P. 28-31.

2. Gurevich V.I. Microprocessor protection relays: in search of optimality // Energy and Industry of Russia. 2009. No 21 (137), November.

3. Gurevich V.I. A new concept for building microprocessor relay protection devices // Components and Technologies. 2010. № 6. P. 12-14.

4. Zakharov O.G. Manipulation of "issues" in relay protection // Power Engineering and Fuel and Energy Complex. 2010. № 2. P. 47.

5. Zakharov O.G. Reliability of digital relay protection devices. Indicators. Requirements. Assessments : a practical guide. Moscow : Infra-Engineering, 2014. 128 p. ISBN 978-5-9729-0073-2 ; Direct Academy : websait. URL: https://biblioclub.ru/index.php?page=book&id=234786 (date of access: 04.21.2021).

6. Bulychev A., Nudelman G. Relay protection. Improvement through proactive functions // Electrical Engineering News. 2009. No 4 (58). P. 30-33.

7. Kamel T.S., Hassan M.A., El-Morshedi A. Application of artificial intelligence systems in remote protection of a power transmission line // Abstracts of the Second International Scientific and Technical Conference "Modern trends in the development of relay protection systems and automation of power systems", Moscow, September 7-10. Moscow, 2009.

8. On the issue of designing and operating microprocessor relay protection devices / A.V. Sychev L.I. Evminov, V.V. Kurganov, A.N. Guminsky // Bulletin of the Sukhoi State Technical University: scientific and Practical journal. 2009. №. 4. P. 73-79.

9. Bestemyanov P.F. Methods of ensuring the safety of hardware means of microprocessor-based train traffic control systems // Electrical Engineering. 2020. №. 9. P. 2-8.

10. Tilk I.G., Lyany V.V., Abakumov M.V. Microprocessor centralization system MPC-I // ZHDM. 2007. № 1. P. 63-66.

11. Synthesis of a controlled majority element circuit for redundant control systems / R.S. Kuliyev, S.N. Sytsevich, Zh.Zh. Zhaboev, I.I. Taukenov // Modern high-tech technologies. 2016. № 9-1. P. 63-66.

12. Shiryaev M.I., Lavrov K.Yu., Andreeva O.N. Improving the method of increasing the reliability of special software for embedded systems // Neurocomputers: development, application. 2014. № 5. P. 38-45.

13. Gasselberg V.S., Sinelshchikov A.V. The use of microcontrollers in devices with increased reliability // Vestnik ASTU. Series: Management, computing technology and informatics. 2011. № 1. P. 108-113.

14. Tipikina A.P., Pevtsova L.S. Evaluation of the software reliability of microprocessor relay protections. DOI 10.15862/74TVN215) // Online journal Naukovedenie. 2015. Vol. 7. № 2. http://naukovedenie.ru/PDF/74TVN215.pdf (access is free). Cover from the screen.

15. Shcherbakov K.S., Shcherbakov S.A. Features of the FreeRTOS real-time operating system // Itech. The Journal of Intelligent Technologies. 2011. № 18. P. 71-77.

16. Goma H. UML-design of real-time systems of parallel and distributed applications // DMK-Press 2011. 704 p. ; National Instrument : What is a Real-Time Operating System (RTOS)? / Access mode: http://www.ni.com/white-paper/3938/en/ (date of access: 24.12.2016).

17. Nazarov S.V. Barsukov A.G. Architecture and reliability of operating systems // Modern information technologies and IT education. 2018. № 1. P. 38-51. URL: http://elib.fa.ru/art2018/bv2476.pdf. (date of access: 24.12.2016).

18. Zamani M.A., Sidhu T.S., Yazdani A. A protection strategy and microprocessor-based relay for low-voltage microgrids. DOI DOI 10.1109/TPWRD.2011.2120628 // IEEE transactions on Power Delivery. 2011. № 26 (3). P. 1873-1883.

19. Hambarde P., Varma R., Jha S. The survey of real time operating system: RTOS // 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies. 2014. January. P. 34-39.

20. Brown G. Discovering the STM32 microcontroller. 2012. № 3 (34). P. 64.

21. Kröning M.W. Concurrency Techniques and Hardware Abstraction Layer Concepts for Embedded Systems in Rust : Doctoral dissertation. Universitätsbibliothek der RWTH. Aachen, 2023.

22. Pham, H. System software reliability. Cham (ZG). Springer Science & Business Media, 2007. 454 p.

23. Laprie J.C., Kanoun K. Software reliability and system reliability // Handbook for Software Reliability Engineering, 1996. P. 27-69.