ПЕРЕПЕЛИЦА СТАНИСЛАВ АНАТОЛЬЕВИЧ

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО ИЗМЕРИТЕЛЬНЫХ СИСТЕМ В ЗАДАЧАХ ЗАЩИТЫ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

АВТОРЕФЕРАТ

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Прогресс во многих областях науки и техники на сегодняшний день невозможен без совершенствования информационно-измерительных систем (далее ИИС), развитие которых идет, в частности, по пути создания распределенных интеллектуальных ИИС. Построение этих ИИС требует комплексного исследования вопросов организации надежного взаимодействия между компонентами системы и поиска эффективных алгоритмов цифровой обработке сигналов (далее ЦОС), применяемых для обработки измерительной информации. Перспективным направлением в данной области является развитие сетевых технологий, ранее применяемых в компьютерных локальных вычислительных сетях. В частности, применение IP-сетей позволит сократить как стоимость системы в целом, так и время разработки. Исследование параметров сетей общего назначения, критически важных для распределенных ИИС и систем управления, позволит внедрить эти сетевые технологии в новых областях применения.

Сегодня ИИС используются в самых разнообразных отраслях промышленности. Применение ИИС в системах защиты энергетических объектов, где в настоящее время интенсивно развивается направление, связанное с использованием микроконтроллеров, привлекательно, прежде всего, тем, что благодаря применению ЦОС, гарантируется высокая стабильность и повторяемость параметров устройств защиты. Более того, при этом может быть обеспечена всесторонняя диагностика, быстрота и наглядность настройки системы.

Возросшие требования по эффективности, предъявляемые к средствам защиты, в настоящий момент сложно обеспечить традиционными методами противоаварийной автоматики. Об интересе к практическим и теоретическим аспектам применения современных ИИС в системах защиты в электроэнергетике и, в частности, для защиты генераторов, свидетельствует существенно возросшее количество публикаций, а также государственная целевая научно-техническая программа “Повышение надежности, экономичности и экологичности энергетической системы России“.

Настоящая работа посвящена развитию распределенных интеллектуальных ИИС, основанных на сети микроконтроллеров, для применения в задачах защиты энергетических объектов, что позволяет реализовать сложные нелинейные алгоритмы защиты генераторов, то есть обеспечить те функции, которых не хватает существующим средствам защиты.

Цель работы

Целью настоящей диссертационной работы является исследование и развитие принципов построения интеллектуальных распределенных ИИС, используемых в защитных системах энергетических объектов, а также разработка общего подхода к проектированию данных систем на основе применения современных технологий информационного обмена.

В связи с поставленной целью в диссертационной работе решены следующие задачи:

1. Изучены и систематизированы вопросы применения ИИС в задачах защиты энергетических объектов и показана специфика таких систем.
2. Разработано и исследовано функциональное разделение системы в проекции на сеть микроконтроллерных защитных узлов (МЗУ). Исследованы алгоритмы цифровой фильтрации измерительного сигнала, специфические для задач защиты энергетических объектов и удобные для реализации на микроконтроллере.
3. Предложена архитектура построения программного обеспечения МЗУ, позволяющая обеспечить высокую надежность системы благодаря реализации технологии “плавного отказа“.
4. Исследована задержка передачи пакетов по стандартной сети Ethernet, построена статистическая функция распределения задержек пакетов для различных типов трафика.
5. Выполнено сравнение стандартных сетей Ethernet и CAN по критериям задержки передачи и вероятности блокировки пакетов.
6. Предложен и практически реализован на микроконтроллере общего назначения частичный стэк протоколов TCP/IP.

Методы исследования:

Теоретические исследования выполнялись с использованием методов спектрального анализа, теории информации и кодирования, теории вероятностей, теории передачи данных, объектно-ориентированного анализа.

Проведение экспериментов происходило с применением имитационного моделирования дискретных систем, управляемых событиями и программирования.

Научная новизна:

1. Предложен метод повышения надежности некритических функций ИИС для защиты энергетических объектов, путем применения специального распределительного сервиса в сети передачи данных.
2. Впервые исследованы задержки сети Ethernet в конфигурации, типичной для распределенной ИИС, выполнено сравнение этого случая с обычной конфигурацией сети Ethernet.
3. Предложена и исследована усовершенствованная архитектура и алгоритм распределенной интеллектуальной ИИС, применяемой в задачах защиты энергетических объектов, основанной на протоколах передачи данных сетей общего назначения.

Практическая значимость:

1. Найдены цифровые фильтры с простой весовой функцией, дающие существенный выигрыш в скорости вычисления спектральных характеристик входных сигналов измерительной системы, при этом решающие поставленную задачу фильтрации с допустимой точностью.
2. Получена кривая статистической функции распределения (СФР) для задержек при передаче пакетов по сети Ethernet, для трех типов трафика: синхронного, имеющего распределение Пуассона и смешанного. График СФР позволяет оценить вероятность доставки пакета при данной задержке или, наоборот, оценить задержку при заданной вероятности. Данное исследование открывает возможность применения сети Ethernet в распределенных системах мягкого реального времени.
3. Разработан и проанализирован способ улучшения характеристик задержки доставки пакетов синхронного трафика для сети Ethernet. Способ заключается в введении небольшой случайной задержки перед отправкой пакета. Задержка изменяет характеристики трафика и делает его похожим на трафик Пуассона, что снижает среднюю задержку на 27%, а задержку 99% вероятности доставки - на 47%.

4. Создан действующий прототип ИИС, где впервые выполнены две реализации частичного стэка TCP/IP: для минимальной и расширенной конфигурации системы.

На защиту выносятся следующие положения:

1. Структура и алгоритм интеллектуальной распределенной ИИС, основанной на протоколах передачи данных сетей общего назначения для применения в задачах защиты энергетических объектов.
2. Способ повышения надежности распределенной ИИС для защитной системы путем функционального разбиения алгоритма обработки измерительного сигнала и реализации “плавного отказа”.
3. Методика применения стандартных сетей Ethernet и CAN и протоколов стэка TCP/IP в распределенных ИИС для защиты энергетических объектов.

Апробация работы:

Основные результаты работы докладывались на Молодежной научно-технической конференции в рамках недели науки (СПбГТУ, 2001).

Публикации:

По теме диссертации опубликовано 3 статьи и тезисы доклада на конференции.

Структура и объем работы:

Диссертация содержит 102 страницы основного текста, введение, 4 главы, заключение, список литературы, приложение.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность проблемы, определяется предмет исследования, формулируется цель и задачи исследования.

В первой главе определяется современный уровень и тенденции развития ИИС, анализируются проблемы создания распределенных интеллектуальных защитных систем энергетических объектов.

На сегодняшний день, при построении ИИС, наблюдается тенденция к интеллектуализации датчиков и к переходу к децентрализованному способу обработки информации. Такая тенденция объясняется тем, что распределенные

системы имеют значительную вычислительную мощность за счет распараллеливания процесса обработки и повышенную отказоустойчивость за счет исключения полного отказа при выходе из строя одного компонента системы. Однако, архитектура и алгоритмы распределенных ИИС усложняются. На данный момент однозначно не решен вопрос о роли сетей передачи данных и о способе представления распределенных алгоритмов в таких ИИС.

В гл.1 также проведен обзор возможных применений ИИС в электроэнергетике и приведена структура энергетической системы (ЭС). Перспективность применения ИИС в задачах защиты энгергетических объектов объясняется возможностью применить общий подход при проектировании защитной системы сначала для одного компонета ЭС и развить его в последствии для целого уровня ЭС, используя на каждом из них алгоритмы, специфические для данного уровня. В данной работе будут рассматриваться вопросы применения ИИС для защиты генератора, как самого ответственного и дорогого компонента ЭС.

Устройства защиты генераторов выпускаются и предлагаются на российском рынке несколькими отечественными и зарубежными электротехническими фирмами. Эти устройства представляют собой многоканальные ИИС (минимально 6 каналов) предназначенные для измерения сигналов переменного тока промышленной частоты (50 Гц). У предлагаемых систем наблюдается два подхода к проектированию. Первый является модернизацией имеющегося оборудования с применением микропроцессорной техники, однако при этом наследуются сложные системы коммутации и трудности организации взаимодействия между компонентами защитной системы. Второй подход, предполагает применение сосредоточенной однопроцессорной ИИС и является развитием первого. Он также имеет ряд существенных недостатков: ограниченные возможности по наращиванию функций системы связанные со сложностью реализации разнородных алгоритмов обработки информации в рамках одного процессора, недостаточная надежность связанная с возможностью полного отказа при выходе из строя одного компонента.

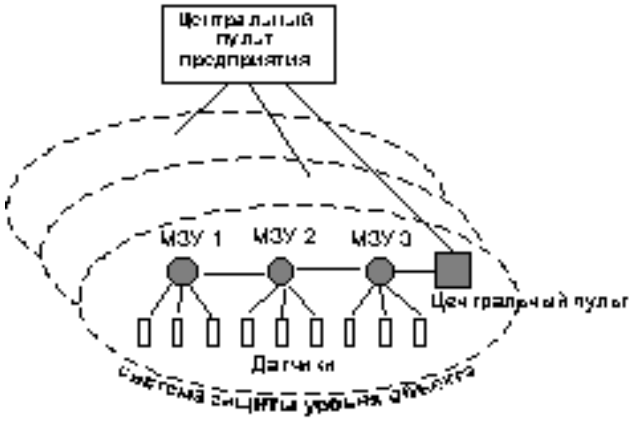
В гл.1 отмечается ряд факторов в пользу применения распределенной многопроцессорной ИИС для защиты энергетических объектов:

- Источником возникновения неисправности в ЭС может служить как отдельный объект системы, так и вся система в целом, при этом неисправность

проявляется в виде сложной комбинаторной задачи (требуется анализ большого количества данных от разных источников и перебор большого количества вариантов, поэтому лучше применить несколько контроллеров).

- Защитные системы, отслеживающие неисправности системного уровня, должны уметь работать с рядом типовых энергетических объектов (генератор, двигатель), обеспечивая непосредственную диагностику состояния этого объекта (требуется специфическая библиотека алгоритмов обработки сигналов и алгоритмов защиты для разнородных объектов ЭС).
- При реализации системы защиты распределенного объекта ЭС требуется при сохранении принципа распределенности сложного алгоритма защиты по нескольким контроллерам, территориальная распределенность ИИС, которая достигается путем взаимодействия контроллеров через внутреннюю сеть.

Далее в гл.1 проводится обзор архитектур построения распределенных интеллектуальных ИИС, анализируются достоинства и недостатки каждой из них. Делается вывод, что наиболее подходящей архитектурой ИИС для защиты энергетических объектов является гибридная архитектура, сочетающая в себе принципы построения иерархической и гетерархической систем. В выбранной архитекуре ИИС основным устройством, обрабатывающим измерительную информацию является микроконтроллерный защитный узел (далее МЗУ). Защитные алгоритмы для различных компонентов ЭС обычно сложны, поэтому в реализации алгоритма участвуют несколько МЗУ. Параметры, вычисленные одним узлом, передаются по внутренней сети и используются другими узлами для дальнейшей обработки. Сеть МЗУ образует защитную систему уровня объекта, причем все узлы в такой сети равноправны. Объединение сетей уровня объекта образует систему защиты уровня предприятия (рис. 1). При этом объединение происходит по приципу ведущий-ведомый.



Р и с 1: Структура ИИС для защиты энергетических объектов.

Рассмотрены алгоритмы защиты энергетических объектов на примере генератора, показано, что основными входными параметрами большинства алгоритмов являются симметричные составляющие - токи и напряжения прямой, обратной и нулевой последовательностей, которые будут вычисляться микроконтроллерным защитным узлом на основе измерения мгновенных значений тока и напряжения.

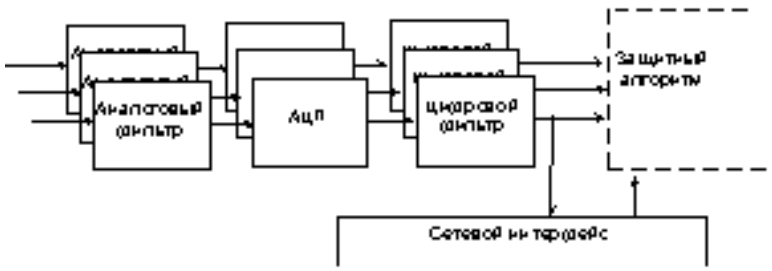
В конце гл.1 показано, что проблематика практической реализации интеллектуальной распределенной ИИС для задач защиты энергетических объектов, определившая задачи данной диссертации, требует рассмотрения следующих вопросов:

- структуры и алгоритмов работы микропроцессорных защитных узлов,
- взаимодействия узлов и, следовательно,
  - способов обеспечения надежности,
  - организации коммуникационной подсистемы и протоколов обмена,
  - способности работы в реальном времени (РВ),
  - интеграции со станционной автоматикой.

Во второй главе

Рассматривается структура тракта обработки измерительного сигнала в МЗУ, исследуются алгоритмы ЦОС, ставится задача фильтрации для ИИС применяемой для защиты энергетических объектов.

Цифровая измерительная подсистема составляет первую часть тракта обработки сигнала в МЗУ (рис 2). Сигнал, снимаемый с измерительного трансформатора тока или напряжения поступает на входной аналоговый фильтр, подвергается аналого - цифровому преобразованию, цифровой фильтрации, преобразованию из мгновенных значений в векторные.



Р и с 2: Структура микроконтроллерного защитного устройства

На втором этапе вычисляются симметричные составляющие, которые используются при реализации различных алгоритмов защиты. При этом алгоритм защиты может быть локальным, т.е. выполняться на основе параметров, вычисляемых тем же узлом, либо распределенным, когда часть параметров алгоритма защиты МЗУ получает по межконтроллерной сети.

В рамках данной работы подробно рассматриваются вопросы совершенствования цифровой фильтрации. Это связано с тем, что именно совершенствование фильтрации в ИИС позволяет достичь существенного выигрыша в быстродействии системы за счет применения фильтров, с характеристиками, наиболее оптимальными для задач защиты энергетических объектов при одновременном учете сопутствующих факторов, связанных с особенностями цифровой фильтрации на микроконтроллерах.

Построение алгоритмов ЦОС на микроконтроллерах требует учета ограниченного количества разрядов представления чисел и приближенного характера некоторых численных методов. При выборе тех или иных численных методов для успешной реализации необходимо выполнение критериев оптимизации: по вычислительной сложности, по затратам оперативной памяти, по скорости выполнения.

Одновременное выполнение всех критериев затруднено по следующими соображениям: реализация алгоритма обработки сигнала возможна, как правило в двух вариантах - рекурсивном и нерекурсивном. Рекурсивные алгоритмы оптимальны с точки зрения количества занимаемой памяти, т.к. промежуточные результаты вычислений хранятся в той же самой области памяти, что и конечный результат. Нерекурсивные алгоритмы требуют больше памяти для хранения входных и выходных данных, но при этом они более быстрые.

Рассмотренные в гл.1 алгоритмы защиты построены на анализе симметричных составляющих. Для вычисления симметричных составляющих выполняется предварительная цифровая обработка измерительного сигнала - фильтрация основной гармоники промышленной частоты (50 Гц). Предварительная цифровая обработка не зависит от специфики защищаемого компонента ЭС и является лишь частью всего алгоритма обработки измерительного сигнала.

Для преобладающей резистивно - индуктивной модели ЭС токи и напряжения возникающие в момент аварии, имеют вид синусоид смещенных постоянным уровнем, затухающим по экспоненте. Смещение существенно проявляется на сигналах токов и незначительно на сигналах напряжения. Помимо смещения, на аварийный сигнал накладываются гармоники промышленной частоты.

Типичным для ИИС входным сигналом является сигнал вида:

(1.1) ,

$$x(t) = x_m(\cos(\omega_0 t - \varphi) - \cos\varphi e^{-\beta t})$$

где

$x_m \cos(\omega_0 t - \varphi)$ - полезный сигнал;

$x_m \cos\varphi e^{-\beta t}$ - помеха,

β - коэффициент затухания,

x_m - амплитудное значение,

φ - начальная фаза.

Задача фильтрации формулируется как извлечение из послеаварийного сигнала значений токов и напряжений основной гармоники с максимально достижимой точностью и скоростью.

Поэтому к цифровому фильтру предъявляется следующий ряд требований: фильтр должен иметь полосно - пропускающий вид АЧХ на частоте основной гармоники промышленного напряжения (50 Гц) при этом обеспечивать особенно хорошее подавление для постоянного и медленно меняющегося сигналов а также для гармоник; иметь полосу пропускания, обеспечивающую быстрый отклик; быстрое затухание переходных процессов.

Далее проводится сравнительный анализ фильтров, реализующих рекурсивный алгоритм обработки (БИХ - фильтры) и ряда КИХ- фильтров с простой весовой функцией. Исследовано влияние длины импульсной

характеристики фильтра на качество подавления помех в измерительном сигнале. Сравнение фильтров выполнялось по критериям качества подавления гармоник, постоянного и медленно меняющегося сигналов, а также по времени установления при импульсном воздействии на входе. Определен наилучший фильтр для поставленной задачи фильтрации.

Далее в гл.2 приводятся рекомендации по выбору входного аналогового фильтра и рассматривается метод определения мнимой части векторов тока и напряжения с точки зрения вносимой в тракт обработки сигнала задержки. Показано, что от момента возникновения аварии, до установления корректных значений векторов на выходе блока предварительной обработки сигнала, при использовании наилучшего из рассмотренных фильтров, проходит 30мс или 1,5 периода промышленной частоты.

В третьей главе

Анализируются вопросы обеспечения надежности распределенной ИИС для защиты энергетических объектов. При этом, рассматриваемым способом достижения надежности является автоматическая реконфигурация, что выдвигает ряд требований к структуризации программного обеспечения микроконтроллерного защитного узла (МЗУ).

Традиционно, устойчивость к сбоям базируется на избыточности, которая подразумевает использование дополнительных ресурсов для детектирования, коррекции или маскировки эффектов, вызванных отказом.

Распределенные ИИС, при всех привлекательных сторонах, имеют недостаток: большое количество узлов в распределенной системе увеличивает вероятность выхода из строя по крайней мере одного узла. Этот недостаток можно устранить путем организации взаимодействия между узлами и разделения функциональности системы. Для обеспечения критических функций системы надежность может быть обеспечена дублированием, для некритических - путем реализации плавного отказа. Выход из строя любых компонентов распределенной ИИС, поддерживающей плавный отказ, проявляется только в виде снижения функциональности.

Для реализации плавного отказа в распределенной ИИС защиты энергетических объектов, необходимо придерживаться следующего порядка проектирования системы:

- определить системные требования вместе с ассоциированными служебными функциями (критически важные функции являются обязательными, прочие имеют заданные уровни утилитарности), которые задают сетку функциональных возможностей ИИС,
- установить системные ограничения, такие как требования выполнения определенных функций в реальном времени,
- выделить абстрактные функциональные блоки, которые удовлетворяют требованиям (с соответствующими программными модулями),
- предоставить аппаратные ресурсы, включая микроконтроллерные узлы и соединяющие их сети,
- установить взаимосвязь между программными и аппаратными ресурсами.

Таким образом, мы получаем некоторую динамическую архитектуру, которая имеет в данный момент оптимальную конфигурацию, и включает выбранное подмножество программных модулей, размещенных в доступных аппаратных ресурсах.

В данной главе проводится разбиение защитных алгоритмов на программные модули, которые представляют собой функционально полные блоки мобильного кода. Данные блоки хранятся в библиотеке и размещаются в МЗУ под управлением менеджера конфигурации для реализации конкретного защитного алгоритма.

Далее, в гл.3 разрабатывается функциональная схема и алгоритм работы менеджера конфигурации.

В четвертой главе

Проводится исследование сети передачи данных, объединяющей МЗУ.

В начале гл. 4 дается обзор сетевых решений. Выделено два класса сетей: с разделяемой средой передачи и без таковой. Все современные высокоэффективные сети передачи данных используют разделяемую среду передачи. Доступ к среде передачи осуществляется на основе протокола.

Мы определили в качестве фундаментальных следующие протоколы доступа к разделяемой среде передачи:

- Опрос (MS/TP)
- Разделение во времени (TDMA)
- Маркерное кольцо (TokenRing)
- Маркерная шина (TokenBus)

- Побитный арбитраж (Bitwise)
- Контроль несущей и определение столкновений(CSMA/CD)

На основе фундаментальных протоколов была построена генеалогия наиболее популярных стандартных сетевых протоколов. Для дальнейшего исследования были выбраны сети Ethernet и CAN.

Ethernet обладает несколькими очень важными свойствами, которые делают его идеальным для применения в надежных распределенных ИИС. Во-первых, это полностью децентрализованный протокол. Нет центральной станции, которая может выйти из строя. Нет маркера, который может быть потерян. Скорость передачи информации 10Мбит/с, что на порядок выше, чем у других протоколов для распределенных систем. Коммуникационное программное обеспечение может разрабатываться и тестироваться на обычных персональных компьютерах, а затем переноситься на микроконтроллер практически без модификаций.

Сеть CAN имеет эффективный механизм разрешения столкновений и разрабатывалась специально для применения в качестве сети микроконтроллеров.

Тестирование свойств сетей происходило с помощью трех типов сетевого трафика, которые характерны для распределенных ИИС: трафик с распределением Пуассона, синхронный трафик и смешанный трафик

Были выполнены оценки задержек для шинной топологии и нагрузке 1 Мбит/с.

По кривой СФР для трафика Пуассона можно утверждать, что практически все пакеты доставляются за время не превышающее 30 пакетов. Из-за отсутствия синхронизации в трафике Пуассона столкновения происходят редко и быстро устраняются алгоритмом отката. Эта ситуация соответствует наилучшему реальному случаю в сети Ethernet, поэтому СФР для данного случая близка к идеальной. Идеальная СФР представляет собой ступеньку из 0 в 1 в момент времени, равный нормализованному времени передачи одного пакета. В этом случае столкновения полностью отсутствуют и все пакеты доставляются за время, необходимое для физической передачи всех битов пакета на данной скорости. Смешанный и синхронный трафик содержат периодические пакеты, поэтому СФР имеет большее отклонение от идеальной.

Основная проблема сети Ethernet - значитльное время доставки пакетов синхронного трафика. Результаты моделирования показывают, что примерно для половины пакетов синхронного трафика, происходит попытка повторить передачу немедленно после столкновения, другая половина откладывается на 51.2 мкс. Столкновения возникают снова как для группы, выполняющей повтор немедленно, так и для группы, отложившей повтор. Цикл столкновений и откладываний передачи будет повторятся для пакета до тех пор, пока он не займет канал или не превысит счетчик числа повторов.

Суть предлагаемого улучшения состоит в следующем: необходимо уменьшить количество одновременно сгенерированных пакетов, тогда счетчики задержек не достигнут больших значений и общая задержка доставки сократится. Введение случайной задержки уменьшает синхронизм пакетов и предотвращает столкновния.

При правильном выборе величины вносимой задержки, общая задержка доставки первого пакета и других пакетов синхронного трафика может быть уменьшена. Однако, если вносимая задержка будет выбрана слишком большой, то дополнительная задержка сведет на нет улучшение, полученное за счет сокращения числа столкновений. С другой стороны, слишком маленькое значение для вносимой задержки не даст должного эффекта.

Следует отметь, что предлагаемый способ улучшения характеристик сети Ethernet при передаче синхронного трафика не требует вмешетельства в аппаратную часть контроллера Ethernet и не затрагивает протокол доступа к среде передачи.

Результаты проведенного исследования показали, что Ethernet имеет лучшие показатели средней задержки пакета, а 99% пакетов Ethernet доставляется за время, сравнимое с задержкой в сети CAN. Арбитраж на шине CAN позволяет эффективно справляться с ситуацией одновременного прихода множества пакетов, ситуацией сложной для сети Ethernet. Поэтому сеть Ethernet допустимо использовать в ИИС мягкого реального времени, сеть CAN пригодна для ИИС жесткого реального времени при малой доле трафика Пуассона. Эти выводы определили применение в качестве межконтроллерной сети разрабатываемой ИИС технологии CAN, а для объединеия сетей контроллеров в систему защиты более высокого уровня применение технологии Ethernet.

В конце гл. 4 исследуются вопросы интеграции распределенной ИИС с системой АСУ энергетического предприятия на основе применения стандартного стэка протоколов TCP/IP.

В пятой главе

Рассмотрены вопросы практической реализации интеллектуальной распределенной ИИС для применения в задачах защиты генераторов.

Согласно предложенной архитектуре ИИС, в рамках данного проекта требуется реализация нескольких микроконтроллерных защитных устройств и центрального пульта, причем основная идейная нагрузка ложится на центральный пульт.

Выполненный автором проект представляет собой две части: аппаратную и программную. В аппаратной части реализован микроконтроллер с сетевым интерфейсом. Центральный пульт выполнен на микроконтроллере ATMega103 и имеет два интерфейса: для сети Ethernet, выполненный на микросхеме CS8900A фирмы Crystal Semiconductor и для сети CAN, реализованный на микросхеме MCP2510 фирмы Microchip. Для МЗУ требуется только интерфейс сети CAN.

Программная часть центрального пульта описывает реализацию операционной системы реального времени (ОСРВ), выполненной специально для микроконтроллеров стэка протоколов TCP/IP и протоколов обмена по сети CAN. Программная часть МЗУ содержит протокол обмена по сети CAN и отладочную версию алгоритма защиты.

Испытания макета подтвердили корректность результатов, полученных в данной диссертационной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. В диссертационной работе выполнен обзор архитектур построения распределенных ИИС реального времени, пригодных для применения в защите энергетических объектов.

2. Для выбранной архитектуры ИИС, на основании обзора алгоритмов защиты энергетических объектов поставлена задача фильтрации и исследованы реализации цифровых фильтров измерительного сигнала на микроконтроллерах.

3. Предложен и исследован способ повышения надежности распределенной ИИС путем функционального разбиения алгоритмов защиты на блоки и применения автоматической реконфигурации блоков в случае выхода из строя узла системы, названный в работе “плавный отказ“.

4. Проведена систематизация протоколов доступа к разделяемой среде передачи. Проанализированы сильные и слабые стороны каждого из протоколов. Выработаны рекомендации по применению конкретных протоколов в распределенных ИИС.

5. Исследовано поведение сети Ethernet при малых нагрузках и трафике, характерном для распределенных ИИС реального времени. Определена максимальная задержка передачи сообщения при выбранных условиях.

6. Предложен и исследован метод улучшения среднего времени задержки передачи сообщения путем введения небольшой случайной задержки перед отправкой пакета.

7. Исследованы практические вопросы применения протоколов стэка TCP/IP в распределенных ИИС, построенных на микроконтроллерах. Показано, что реализация частичного стэка TCP/IP возможна, даже при малых имеющихся ресурсах и приводит к существенному расширению функциональных возможностей ИИС.

Публикации по теме диссертации

1. Перепелица С.А. "Система ЦУТ: к вопросу об управлении распределенными сетями микроконтроллеров", // "Вестник связи" №3, 1999 г.

2. Перепелица С.А. "Микроконтроллер с сетевыми возможностями", /// Микропроцессорные средства измерений. Вып.2., Сб. науч. тр. С.-Петербург: АО "Нестор", 2001 г.

3. Перепелица С.А. "Реализация быстрого преобразования Хартли на микроконтроллере", //Микропроцессорные средства измерений. Вып.2., Сб. науч. тр. С.-Петербург: АО "Нестор", 2001 г.