Секция «Вычислительная техника и микропроцессорные устройства»

К.Д. Алексеева, А.А. Лазарев
Научный руководитель: канд. техн. наук, доцент А.А. Белов
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Всемирная система объединения компьютерных сетей

Интернет является всемирной системой объединения компьютерных сетей меньшего масштаба. В соответствии с классификацией компьютерных сетей Интернет является крупнейшей глобальной сетью объединяющей на данный момент более 1 миллиарда компьютеров. Количество пользователей сети Интернет из года в год растет, достигнув на начало 2013 года более 2,5 млрд. человек. Множество сервисов, предоставляемых сетью Интернет для своих пользователей, обуславливает столь широкое применение глобальной сети. Более третьей части населений планеты не мыслят своей жизни без использования преимуществ Интернет технологий.

Свою историю сеть Интернет ведет с 1957 года, в момент, когда военное ведомство США осознало необходимость создания и применения высокоскоростной и надежной системы передачи данных. Американское агентство по научным и исследовательским разработкам в области обороны сформировало предложение разработки крупнейшей компьютерной сети. Ведущие научные центры и университеты США приняли участие в разработке и уже к 1969 году вычислительная сеть объединила 4 крупнейших университета страны, получив название ARPANET. С каждым годом сеть Интернет активно росла и развивалась, её использовали не только военные но и учёные из различных областей знаний. Первый Интернет сервер Калифорнийского университета имел громадный по тем временам объем оперативной памяти в 24 Кб. В 1969 году был впервые успешно проведен сеанс обмена сообщениями, поэтому именно этот год считают днём рождения глобальной сети Интернет. В 1973 году к сети Интернет были подключены локальные сети ряда стран Европы – тем самым сеть получила международный статус.

В 1970 гг. сеть использовалась лишь для обмена электронной почтой, и только в концу 1980 гг возникла идея удаленного доступа к информационным ресурсам располагающимся на выделенных Интернет серверах. В 1984 г. была разработана DNS - система доменных имен, в 1988 году – первый чат (IRC-протокол), а в 1989 году Европейским советом по ядерным исследованиям была предложена концепция организации Всемирной паутины WWW (World Wide Web). Данную идею пропагандировал британец Тим Бернерс-Ли, разработавший протокол передачи гипертекстовых документов HTTP, язык веб-разметки документов HTML и идентификаторы веб ресурсов URI. В настоящее время к сети интернет подключена даже международная космическая станция.

Перспективами развития сети Интернет является создание высокоскоростной экспериментальная сети, созданной и поддерживаемой американским консорциумом Интернет2 (Internet2). Сам консорциум является негосударственной некоммерческой организацией и занимается разработкой и внедрением передовых веб-приложений и новейших сетевых и телекоммуникационных технологий. Одной из подобных сетей, относящихся к Интернет2, является сеть «Абилин» уже объединяющая более 230 американских университетов, научных центров и других учреждений. Особенностью сети «Абилин» является высокая скорость передачи данных, теоретически она может достигать 10 Гбит/с, а реальная скорость передачи составляет порядка 7 - 8 Гбит/с. Дальнейшее совершенствование общедоступной сети Интернет многие связывают с внедрением концепции семантической сетевой Интернет паутины, что позволило бы пользователям и компьютерам более эффективно взаимодействовать в процессе создания, классификации и обработки информации.

Н.А. Веденин
Научный руководитель: канд. физ.-мат. наук, доцент М.Н. Кулигин
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Автоматизированная система управления мобильным роботом

В рамках дипломной работы необходимо разработать автоматизированную систему управления мобильным роботом, а также необходимое программное обеспечение. Основной отличительной чертой мобильных роботов является наличие способности к переместительным движениям системы в пространстве. К роботам данного класса относятся роботы, способные самостоятельно преодолевать участки с неровной поверхностью на открытом воздухе или в помещении. Данный тип роботов чаще всего используется в недетерминированных средах.
Проблема разработки автоматизированных систем управления мобильными роботами, их реализации в современных условиях является актуальной и довольно значимой в робототехнике. Её решение во многом зависит от уровня технической компетентности инженера-разработчика, осведомленности в области технической базы, используемой для проектирования и принципов программной реализации.

Любой мобильный робот может быть представлен в виде совокупности трех больших систем - транспортной, специальной и управления [1].

Транспортная система представляет собой транспортное средство, предназначенное для доставки специального и технологического оборудования к месту выполнения поставленной задачи.

Специальные системы служат для непосредственного выполнения поставленных задач. Специальная система состоит из необходимого набора технологического оборудования, состав которого определяется видом решаемой задачи и назначением мобильного робота. Например, при решении разведывательных задач технологическим оборудованием является комплект датчиков и средства первичной обработки информации. Выполнение технологических задач может обеспечиваться манипулятором и набором сменного инструмента к нему. При проведении взрывотехнических работ необходимым оборудованием являются средства диагностики взрывных устройств и гидроразрушители.

Система управления обеспечивает управление движением и работой технологического оборудования, а также адаптивное управление ходовой частью и энергетической установкой с учетом взаимодействия транспортной системы с окружающей средой.

Система управления включает в себя следующие подсистемы:

- информационно-управляющую часть (аппаратура управления роботом, датчики, система технического зрения и микроконтроллер (микроконтроллеры) предварительной обработки информации), расположенную на мобильном роботе;
- пост оператора мобильного робота (пульт управления, видеопросмотровые устройства, ЭВМ для обработки информации);
- комплект приемо-передающей аппаратуры, обеспечивающей передачу информации от робота на пост оператора и управляющих команд от поста оператора на мобильный робот.

В рамках данной дипломной работы необходимо разработать только информационно-управляющую часть общей системы управления:

- обобщённую структурную схему системы управления мобильным роботом;
- выбрать соответствующую структурной схеме элементную базу и разработать схемы её отдельных блоков;
- разработать протоколы взаимодействия между отдельными блоками системы управления роботом и соответствующее этим протоколам программное обеспечение.

Особенности программного обеспечения систем управления роботом.

Программирование систем управления роботом в значительной степени отличается от программирования классических задач для микроконтроллера. Программирование робота должно быть, специализировано и адаптировано для его поведенческой модели, отличающейся

от поведенческой модели человека именно по причине его мобильности. Классические алгоритмические методы трудно использовать при программировании роботов в силу большой сложности математических моделей, их описывающих.

Родни Брукс из Массачусетского технологического института (MIT) стал первым, кто предложил новый подход к программированию роботов. Используя пример насекомых, он предложил свести к минимуму процесс мышления, предшествующий действию. Свой алгоритм поведения робота Брукс назвал «Архитектурой приоритетных взаимодействий» [2]. Архитектура приоритетных взаимодействии позволяет собрать в единую согласованную (когерентную) систему все элементы управления мобильным роботом. Преимущество этого способа, объединяющего восприятие и движение, заключается в том, что он требует лишь незначительных математических ресурсов.

Литература

1. С. Л. Зенкевич, А. С. Ющенко. Основы управления манипуляционными роботами. — М: МГТУ им. Н. Э. Баумана, 2005.

2. Сборка и программирование мобильных роботов в домашних условиях / Ф. Жимарши, пер. с фр. М. А. Комаров. - М.: НТ Пресс, 2007. - 288 с.

С.В. Гусенков
Научный руководитель: преподаватель К.В. Мортин
Государственное бюджетное образовательное учреждение среднего профессионального образования Владимирской области "Муромский техникум радиоэлектронного приборостроения"
г.Муром, ул. Комсомольская, д. 55
E-mail: mortinkv@ya.ru

Аппаратно-программный комплекс шифрования данных с использованием серверного и сервисного набора ключей передаваемых по защищенному каналу

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-дешифрования. В соответствии со стандартом ГОСТ 28147-89[1] под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований [2 с. 31 - 34]: достаточная крипто- стойкость (надежность закрытия данных), простота процедур шифрования и де- шифрования. Данным требованиям, в какой-то степени отвечают следующий ряд алгоритмов: Шифр Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом, шифрующие таблицы Трисемуса, биграммный шифр Плейфера, система шифрования Вижнера, шифр «двойной квадрат» Уитсона, шифрование методом Вернама [2].

Данные алгоритмы имеют множества недостатков:

-подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного и отрытого текста, сохраняется алфавитный порядок в последовательности заменяющих букв, число возможных ключей мало, возможность взлома шифротекста на основе анализа частот появления букв.

Разработанное по комплексному методу программное обеспечение, работает по следующему принципу:

Заносим ключ в буфер, загружаем первый ключ (ПИН КОД) и выбирает ключ из набора 10 ключей.

Определяем тип символа, присваиваем алфавит использования при шифровании данных, если тип алфавита русская буква, загружается второй ключ из набора, который определяет порядок запуска алгоритма. Номер символа ключа равен остатку деления количества символов во втором ключе на номер шифруемого символа, затем выбираем алфавит, определяем какой ключ для алгоритма будет использоваться, а номер ключа вычисляется по следующему закону: начальное значение ключа + номер в диапазоне действующих ключей, для данного алгоритма. Выбираем алгоритм, если 1 берем значение ключа из диапазона ранее найденного и применяется модернизированный алгоритм Цезаря, если 2 и русский язык - символ кодируется алгоритмом Трисимуса, если алфавит английский, то используется алгоритм Вижнера, если 3 и русский алфавит используется алгоритм Цезаря с гаммированием, если алфавит выбран английский то используется алгоритм Цезаря с ключевым словом, если 4 используется алгоритм Вижнера, если 5 и алфавит языка русский используется Цезарь гаммирование, а если английский алфавит , то алгоритм Цезаря, если 6 используется алгоритм Цезаря с ключевым словом.

Достоинства алгоритма GNM:

- высокая крипто стойкость алгоритма от взлома (Защита данных pin кодом);
- большой размер ключа (2,6Кбайт каждый из 10 штук);
- нестатическое шифрование (Одна и та же буква шифруется всегда по -разному);
- высокая система защиты алгоритма (используется фильтр);
- сжатие текста при использовании формата GNM.

Литература

1. Ковалевский В., Максимов В. Криптографические методы. // КомпьютерПресс. - 1993. - N 5. - с. 31-34.
2. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2002.

С.В. Изъюров
Научный руководитель: канд. физ.-мат. наук, доцент М.Н. Кулигин
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Программный комплекс управления периферийными устройствами стенда SDK - 1.1

В рамках НИРС необходимо было разработать программное обеспечение для учебного стенда SDK - 1.1. Назначение разрабатываемого ПО – управление аппаратными ресурсами стенда SDK-1.1 при помощи персонального компьютера через RS-232 интерфейс.

Результаты работы (разработанное ПО) представляют собой учебное программное обеспечение, реализующее взаимодействие двух компонент — учебного стенда SDK-1.1 и ПК через последовательный порт. Реализован протокол с установкой и поддержкой соединения, квитированием некоторых сообщений. Эти особенности обусловлены отсутствием надежной передачи данных на более низком уровне. Кроме того, решается и проблема потери сообщений в случае переполнения буферов.

Программное обеспечение состоит из двух компонент: сервера, реализующего часть для ПК, и клиента, реализующего часть, работающую на SDK-1.1. Для более простой

реализации протокола обмена используется единый исходный код протокола обмена, как для клиента, так и для сервера.

В данной работе учебный стенд задействован как удаленный терминал информационной системы. В качестве устройств подключенных к SDK-1.1 использовались светодиодные индикаторы, жидкокристаллический индикатор (ЖКИ WH1602B-YGK-CP) и клавиатура (AK1604A-WWB) [1]. На рис.1 для примера показаны информационные потоки обмена данными между стендом и компьютером.

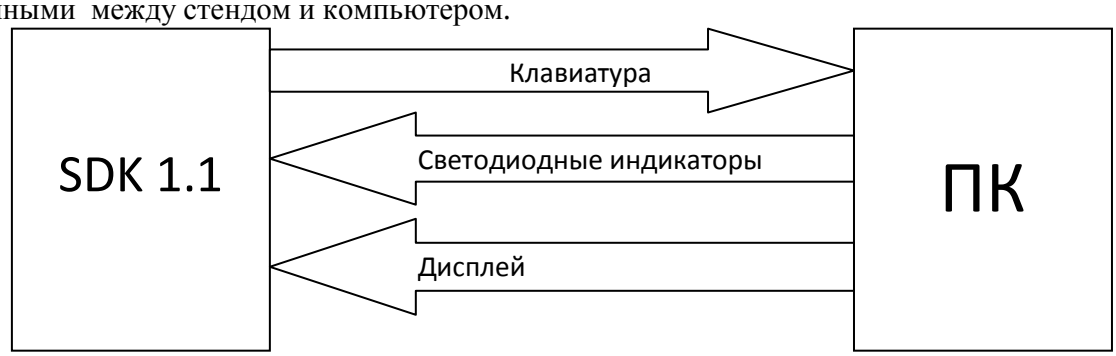


Рис.1. Потоки команд между SDK1.1 и ПК

Таким образом, с помощью разработанного ПО мы можем как управлять любыми устройствами, подключенными к стенду, так и получать от этих устройств необходимые нам данные.

Программа управления представляет собой приложение, написанное с использованием языка Delphi и запускаемое на ПК; разработанный интерфейс позволяет управлять светодиодными индикаторами, выводить сообщения на дисплей, отображать нажатие клавиш на клавиатуре стенда, также позволяет отслеживать приходящие потоки команд.

При разработке протокола взаимодействия использовались базовые понятия протоколов TCP и IRC. Формат сообщения имеет вид «’контрольная сумма’ ‘номер сообщения’ ‘название команды’ ‘параметр’».

Рис.2. Оконный интерфейс программы управления

Литература

1. http://lmt.ifmo.ru/index.php/production/productboards/productsdk11
2. http://embedded.ifmo.ru/index.php/support/sdk-11

К.Е. Лемешкин
Научный руководитель: канд. физ.-мат. наук, доцент М.Н. Кулигин
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Устройство сопряжения абсолютных датчиков углового поворота с ПК

В рамках курсового проектирования необходимо спроектировать функциональный узел (устройство сопряжения) обеспечивающий сбор информации с абсолютных датчиков углового поворота и их отправку по локальной сети на ПК.

Описание принципа действия абсолютного датчика углового поворота

Абсолютные датчики углового положения каждому значению углового положения вала (преобразуемого угла) ставят в соответствие значение числового эквивалента, который формируется на выходе датчика, как правило, в виде сигнала цифрового кода. При этом указанное взаимно однозначное соответствие сохраняется, как при движении вала, так и при его неподвижном положении и не требует возвращения вала в начальную позицию. Таким образом, значение кода не теряется после выключения и включения питания датчика, восстанавливается после прохождения помехи или превышения допустимой скорости вращения вала, ограничиваемой правильным считыванием кода. Приведённые свойства выгодно отличают абсолютные датчики углового положения от инкрементных угловых преобразователей.

Конструктивно абсолютный датчик включает в себя оптико-механический узел, оптико-электронное считывающее устройство, а также электронную схему выделения и обработки сигналов фотоприёмников.

В общем случае, считывающее фотоприемное устройство содержит матрицу пространственно распределённых фотоприемников с установленной перед ними анализирующей маской. Для получения значений кода на один оборот вала, кратных одному угловому градусу, используют укороченный код Грея, начальное значение которого не соответствует нулевой позиции обычного кода Грея, а имеет значение некоторого смещения, позволяющего при замыкании кодовой последовательности сохранить основные его свойства. В зависимости от уровня сигналов, снимаемых с фотоприемников, им присваиваются значения 0 или 1, то есть получаемые кодовые комбинации являются бинарными кодами.

К разрабатываемому устройству предъявляются следующие требования:

- связь с ПК осуществляется по стандарту IEEE группы 802.3 (ethernet);
- протокол сетевого уровня IP;
- протокол транспортного уровня UDP;
- абсолютный датчик ЛИР-ДА158А (использует SSI интерфейс для связи).

Следовательно, необходимо реализовать устройство сопряжения под конкретный датчик: ЛИР-ДА158А. Сбор информации с датчика будет осуществлять микроконтроллер, а затем передавать эту информацию компьютеру. Аппаратно датчик будет связан с контроллером по интерфейсу SSI, а контроллер с компьютером по интерфейсу RS-485. Далее (рис.1) приведена функциональная схема абсолютного датчика углового положения с интерфейсом SSI. Необходимо отметить, что на рис. 1 все элементы находящиеся внутри пунктирной линии реализованы внутри датчика.

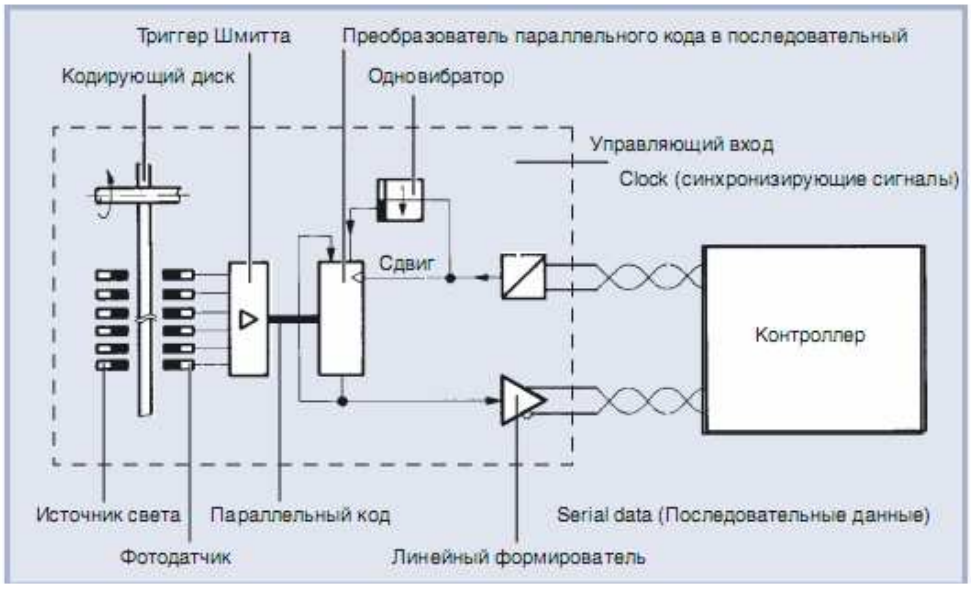


Рис.1. Схема абсолютного датчика углового положения с интерфейсом SSI.

Разрешающая способность датчика ЛИР–ДА158А равна 12 разрядам. Его временные характеристики управления (интерфейса SSI) показаны на рисунке 2.

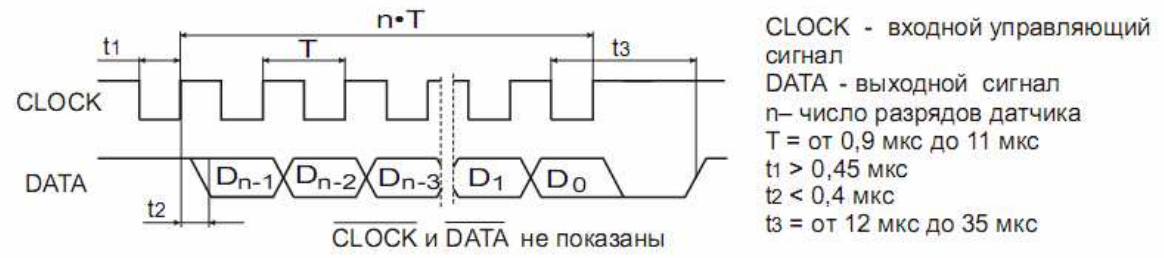


Рис. 2. Временные характеристики интерфейса SSI датчика ЛИР-ДА158А

Организация обмена данными по сети.

Исходя из общего назначения системы, частью которой является и разрабатываемое устройство сопряжения датчиков, можно сделать вывод о том, что максимальное быстродействие сетевой компоненты от устройства сопряжения датчиков не требуется. Следовательно, нет необходимости в использовании специального сетевого контроллера с аппаратной поддержкой IP протокола, достаточным будет использование контроллера с аппаратной реализацией протокола Ethernet. Остальные сетевые протоколы (ARP, IP, UDP, ICMP) могут быть реализованы программно на базе управляющего микроконтроллера.

На основании этих требований было решено использовать следующие микросхемы:

- микроконтроллер ATMega16-16AI, его памяти программ и данных с запасом хватает для реализации алгоритмов управления и сетевых протоколов;

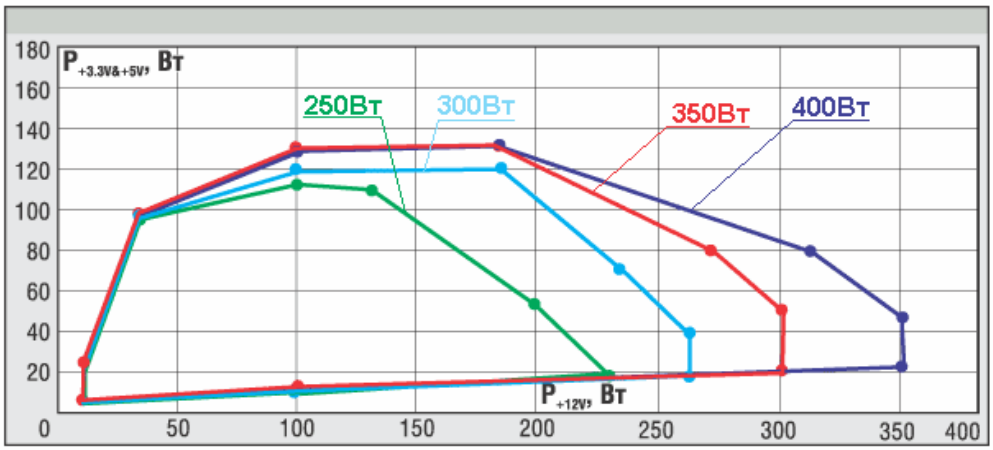
- контроллер Ethernet ENC28J60-I/SO – это один из самых распространённых и отработанных сетевых контроллеров канального уровня, имеет SPI интерфейс для сопряжения с микроконтроллером.

Д.В. Никитин
Научный руководитель: канд. физ.-мат. наук, доцент М.Н. Кулигин
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Тестирование компьютерных блоков питания методом снятия кросс-нагрузочных характеристик

В рамках дипломного проектирования предполагается разработать микроконтроллерную систему (стенд) для проверки заявленных технических характеристик современных компьютерных блоков питания. Цель проекта - разработка аппаратной части и программного обеспечения системы для проверки работоспособности и тестирования блоков питания форм-фактора ATX путём снятия кросс-нагрузочных характеристик (КНХ).

Требования к ATX блокам питания компьютеров стандартизованы и оформлены компанией Intel в документе ATX12V Power Supply Design Guide [1]. В нём вводится понятие Cross Loading Graph (кросс-нагрузочная характеристика - КНХ). На диаграммах, приведённых ниже, показаны требуемые этой спецификацией КНХ для разных по мощности блоков питания (диаграммы заимствованы из [2]).



КНХ имеет вид замкнутой кривой и строится в двумерной системе координат: по абсциссе откладывается значение отдаваемой мощности цепью +12В, по оси ординат -- суммарная мощность по цепям +3,3В и +5В. Физический смысл диаграммы: - в каждой точке, соответствующей определенной отдаваемой мощности и находящейся внутри области, ограниченной указанной кривой, блок питания (БП) обязан обеспечить питание нагрузки стабильными напряжениями с заданными точностью и уровнем пульсаций на выходе.

Бесспорно, главной задачей блока питания является стабилизация выходных напряжений. Поэтому важнейшим из тестов будет тест на проверку отклонения формируемых напряжений от заданных. Следует отметить параметры, которые не следует измерять в процессе тестирования. Это тесты, в которых измеряется максимальная выдаваемая блоком питания мощность – когда в ходе теста нагрузка на блок повышается до момента срабатывания защиты или же просто сгорания блока. Такие тесты дают слишком сильный разброс результатов не только в зависимости от конкретного экземпляра блока, но и в зависимости от того, как именно экспериментатор его нагружает – то есть, как распределяется нагрузка по различным шинам (+12В, +3,3В и +5В) блока.

Требования к разрабатываемому стенду

Данное устройство должно производить измерение основных электрических параметров в выходных питающих цепях БП, их оцифровку и передачу в персональный компьютер для последующей обработки с целью определения характеристик испытуемого блока питания. Одна из первостепенных задач, которые нужно решить, начиная разработку стенда – это как нам тестировать блоки питания на реальной (в качестве нагрузки выступает компьютер) или виртуальной (в искусственных условиях) нагрузке.

Главный и очень большой минус реальной нагрузки в том, что в каждый момент времени мы не знаем потребляемую мощность. Кроме того, при реальной нагрузке получится, что блоки питания или будут работать, или нет, но практически невозможно будет оценить для какой системы подойдет данный блок. Другая проблема - тестирование с реальным компьютером дает интегральный результат - из него нельзя выделить отдельные выходные шины блока питания (+5В, +12В, +3.3В). Но блоки различаются не только по общей, интегральной мощности - у одного блока больше допустимый ток по +3.3В, зато меньше по +12В, чем у другого блока.

В качестве нагрузки можно использовать несколько блоков, набранных из мощных низкоомных резисторов. Но так как в разрабатываемом устройстве управление нагрузкой происходит не вручную, а с помощью микроконтроллера и устройство должно иметь возможность динамически (во время сбора данных) менять нагрузку на выходные цепи тестируемого блока питания, то целесообразно в качестве нагрузки использовать КМОП транзисторы и управлять ими через ЦАП подключенный к микроконтроллеру, за которым идут источники тока, выполненные на усилителях.

Аппаратный состав разрабатываемого стенда включает следующие структурные составляющие:

- вычислительное устройство на базе однокристальной ЭВМ (ОЭВМ). Задача блока состоит в автоматизации управления стендом на всех этапах тестирования вплоть до передачи данных в ПК;
- модуль аналого-цифрового преобразования. Данный блок базируется на трех микросхемах АЦП – по одному АЦП для каждой шины питания;
- модуль цифро-аналогового преобразования. В ходе выполнения программы на ОЭВМ этот модуль преобразует цифровые значения величин тока для управления нагрузкой в аналоговую форму. Основой данного модуля являются три ЦАП.

Литература

1. www.formfactors.org/developer.
2. http://itc.ua/article.phtml?ID=18944

С.Э. Тихонов, В.В. Молотихин
Научный руководитель: канд. техн. наук, профессор Ю.А. Кропотов
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Развитие микропроцессоров INTEL

Компьютер – это устройство, предназначенное для автоматического выполнения последовательных команд в соответствии с заложенной программой. В настоящее время компьютером, как правило, называют персональную электронно-вычислительную машину. Основные компоненты компьютера – центральный процессор, материнская плата, оперативная память, устройства ввода и устройства вывода. Наиболее важным и сложным элементом компьютера является микропроцессор.

Микропроцессор – это устройство, созданное для выполнения алгебраических и логических операций. Является основной частью ЭВМ. Этот компонент определяет быстроту выполнения вычислительных операций и организует согласование и выполнение всех сопутствующих этим вычислениям команд, поэтому и является самой дорогостоящей частью компьютера.

Существует две основные корпорации по созданию микропроцессоров AMD и Intel. Рассмотрим историю развития микропроцессоров на примере процессоров INTEL.

Компания INTEL была основана 1968 году Говардом Мур и Робертом Нойсом. Сейчас производит широкий спектр электронных устройств, компьютерных компонентов, включая микропроцессоры.

В 1970 году был сделан важный шаг на пути к персональному компьютеру. Маршиан Эдвард Хофф сконструировал интегральную схему аналогичным по своим функциям центральному процессору большого компьютера. Так появился первый микропроцессор Intel 4004, который был выпущен в продажу в 1971 г. Для того времени это был настоящий прорыв, тот микропроцессор имел размер менее 3 см и был производительней процессоров 1 поколения.

Позднее был создан усовершенствованный микропроцессор INTEL 8080. Он закладывался как 8 битный чип. У этого процессора было более широкое количество микрокоманд. До конца 70-х Intel 8080 был стандартом для компьютерной индустрии.

В 1979 году фирма Intel выпустила новый микропроцессор Intel 8086/8088. Тогда же и появился первый сопроцессор Intel 8087, а Intel 8088 был выбран как основной 16 зарядный процессор.

В 1985 году появился Intel 8038SX и Intel 8038DX, они открыли класс 32 разрядных процессоров. Новые микропроцессоры работали на частотах 16,20-40 МГц.

В 1989 году Intel выпустил новые микропроцессоры и Intel 80486SX/DX/DX2 имевшие 1.2 млн. транзисторов на кристалле, изготовленному по технологии 1 мкм, отличается от предыдущих наличием на кристалле кэша и встроенного сопроцессора.

В 1993 году появились первые процессоры Pentium с частотой 60-66МГц. Это были 32-разрядные процессоры с 64- битной шиной данных. Спрос к процессору со стороны производителей и покупателей PC сдерживался его очень высокой ценой. Параллельно с Pentium развивался процессор PentiumPro, который отличался новшествами «динамического исполнения инструкций» кроме того, в его корпусе разместили вторичный кэш объемом 256 Кб. В начале 1997 года появились процессоры PentiumMMX. Он предполагал параллельную обработку группы оперндов одной инструкцией. Технология MMX призвана ускорять выполнение мультимедийных приложений, в частности операции с изображениями и обработку сигналов. Технология MMX была соединена с архитектурой PentiumPro – и в мае 1997 года появился процессор PentiumII. Он представляет собой слегка урезанный вариант ядра PentiumPro с более высокой внутренней тактовой частотой.

7 июня 1998 компания Intel представила процессор Celeron с тактовой частотой 300 МГц и снизила цену на ранее выпускавшуюся модель 266 МГц.

Таблица 1. Характеристик процессоров разного поколения.

Intel 1971-1999	**Intel 1999-2002**	**Intel 2002-2012**
Intel® 8004 **Intel® 8080** **Intel® 80186** **Intel® Pentium® (P5)** **Intel® Celeron®**	**Intel® Pentium® III** **Intel® Pentium® III-S** **Intel® Xeon** **Intel® Celeron**	**Intel® Xeon® E7** **Intel Pentium Dual-Core** **Intel® Core™2 Duo** **Intel® Core™ i7**
Тактовая частота: От 108 кГц до 600 МГц Разрядность: От 4 до 32 Технология производства: От 3 мкм до 0,25 мкм	Тактовая частота: От 500 МГц до 2 ГГц Разрядность: От 64 до 64 Технология производства: От 0,25 мкм до 0,18 мкм	Тактовая частота: От 2 ГГц до 3,6ГГц Разрядность: От 64 до 64 Технология производства: От 0,18 мкм до 22 нм

В ближайшие 10-20 лет, скорее всего, изменится материальная часть процессоров ввиду того, что технологический процесс достигнет физических пределов производства. Возможно, это будут:

Оптические компьютеры – это компьютеры, в которых вместо электрических сигналов обработке подвергаются потоки света (фотоны, а не электроны).

Квантовые компьютеры – это компьютеры, работа которых всецело базируется на квантовых эффектах. В настоящее время ведутся работы над созданием рабочих версий квантовых процессоров.

Молекулярные компьютеры – вычислительные системы, использующие вычислительные возможности молекул (преимущественно, органических). Молекулярными компьютерами используется идея вычислительных возможностей расположения атомов в пространстве.

Литература

1. Гук М. Процессоры PENTIUM II, PENTIUM PRO и просто PENTIUM. – СПб.: Питер, 1999.
2. Джексон Т. Intel: взгляд изнутри. – М.: Лори, 1998.
3. Рудометов Е. Материнские платы и чипсеты. – СПб.: Питер, 2007.

Д.О. Шмельков
Научный руководитель: старший преподаватель Д.В. Бейлекчи
Муромский институт (филиал) Владимирского государственного университета
Владимирская обл., г. Муром, ул. Орловская, д.23
E-mail: kaf-eivt@yandex.ru

Разработка алгоритмов и программного обеспечения шифрования файлов для микропроцессора архитектуры ARM-CortexM3

В информационном обществе информация стала частью нашей жизни. Каждый из нас имеет устройство для хранения данных - карту памяти или USB флеш-диск. Мы можем иметь при себе гигабайты данных. Зачастую эти данные не имеют никакой ценности, но, если выполняется работа с очень важными документами или базой данных, встаёт вопрос о том как защитить эту информацию. Можно воспользоваться средствами компьютера и специальным программным обеспечением, но что делать, если его под рукой не оказалось? Для этого необходимо использовать средства микропроцессорной техники - микроконтроллеры. Современные однокристальные процессоры позволяют, не только полностью справится с поставленной задачей, но и построить на их базе устройство для шифрования/дешифрования файлов без участия компьютера. Стоит так же учитывать то, что использование микроконтроллеров для решения этой задачи также налагает некоторые ограничения на используемые алгоритмы, поддерживаемую файловую систему и устройства. Рынок подобных устройств не очень велик, что естественно предлагает нам свободу для создания новых устройств.

Таким образом, существует необходимость в разработке алгоритмов, устройств и программного обеспечения позволяющих осуществлять шифрование и дешифрование файлов, как с использованием компьютера, так и без его непосредственного участия.

Устройство для шифрования должно включать в себя: разъем для подключения устройства хранения информации, и разъём для подключения к персональному компьютеру.

Программа, управляющая микропроцессором, должна обнаруживать наличие/отсутствие устройства хранения данных, производить простейшие операции с файловой системой, выполнять шифрование и дешифрование файлов (всех сразу и в отдельности), принимать/отправлять команды и данные с компьютера и на компьютер.

Программное обеспечение персонального компьютера должно посылать данные и команды для вывода списка файлов, автоматического шифрования/дешифрования всех файлов, шифрование/дешифрование отдельных файлов, копирования файлов и поиска файлов. Программа принимает от устройства данные о структуре файловой системы, списки файлов и содержимое файлов.

На основе анализа поставленной задачи было принято решение использовать процессор ARM Cortex-M3. Процессоры архитектуры ARM (Advanced RISC Machine) являются достаточно производительными по сравнению с другими архитектурами процессоров и имеют низкое энергопотребление по сравнению со многими аналогичными процессорами. Одним из представителей этой архитектуры является процессор ARM Cortex-M3. Данный процессор работает на частоте 72 MHz, имеет в своём составе 7 модулей таймеров/счётчиков, 3 модуля USART, 3 шины I2C, поддерживает интерфейс SDIO. ARM Cortex-M3 содержит 32-х разрядные регистры что соответственно упрощает работу с большими числами и поэтому имеет преимущество перед 16-ти и 8-ми разрядными контроллерами. Так же стоит отметить то, что рыночная стоимость этого процессора колеблется на уровне стоимости менее производительных 16-ти и 8-ми разрядных контроллеров.

В ходе исследования популярных устройств хранения информации был выбран тип поддерживаемых устройств, такие как карты памяти microSD, а так же интерфейс для связи с ними – SDIO. Интерфейс SDIO обеспечивает скорость передачи данных до 4 Mbit/s и соответственно увеличивает производительность работы. Устройство так же должно осуществлять взаимодействие с компьютером, было принято решение использовать для связи интерфейс USB, реализующий виртуальный COM порт.

Для отладки программы решено использовать отладочную платформу STM32, так как выбранная отладочная платформа включает в себя все нужные интерфейсы.

На данный момент одной из самых оптимальных файловых систем, по критериям производительности и экономии рабочего ресурса карт памяти, является система FAT32. Поэтому именно работу с этой системой будет поддерживать разрабатываемое программное обеспечение. Симметричные алгоритмы позволяют осуществлять надёжное шифрование/дешифрование данных с использование ключей: различного формата, различного набора символов и различной длины. Из всех симметричных алгоритмов был выбран метод гаммирования, данный метод является самым производительным по сравнению с остальными, обладает высокой криптографической стойкостью и простой программой реализацией, эти параметры в рамках поставленной задачи является немаловажным фактором. При дешифровании файлов мы должны обеспечивать проверку подлинности введённого ключа для этого мы использовали алгоритм получения CRC32, он позволяет получать уникальные идентификаторы для файлов и уменьшает вероятность совпадения CRC кодов.

Разработана структурная схема аппаратно-программной системы и функциональная схема программного обеспечения, на основе которых было разработано программное обеспечение на языке C для архитектуры ARM и для персонального компьютера на языке Delphi, реализующее алгоритмы описанные выше. Общая структурная схема, реализующая поставленную задачу, приведена на рис. 1.

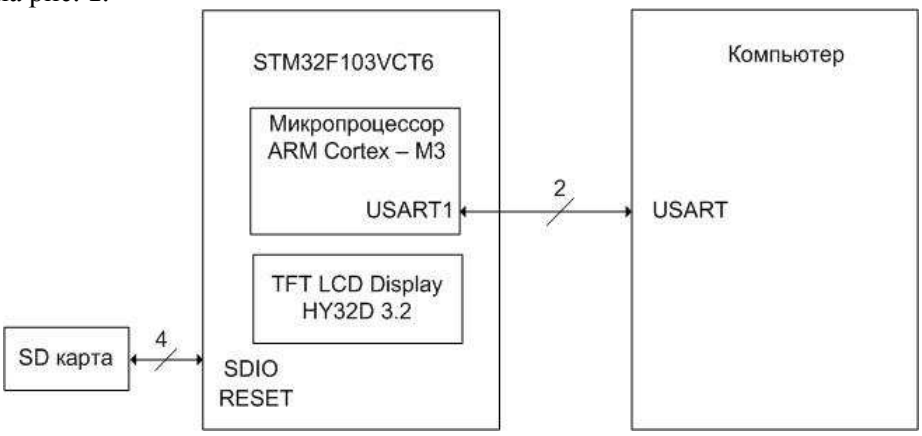


Рис. 1. Общая структурная схема аппаратной части системы

Таким образом, в результате работы было разработано устройство и программное обеспечение, которое позволяет осуществлять шифрование/дешифрование файлов файловой системы FAT32 на базе микроконтроллера ARM Cortex-M3 с использованием симметричного алгоритма шифрования. Так же было написано вспомогательное программное обеспечение. Разработанная система обеспечивает возможность защиты данных при хранении их на флеш-картах.