RFID –это просто. Реализация собственного RFID транспондера и ридера.

После нескольких лет работы по RFID тематике и разработки разнообразных считывателей для моделей транспондеров популярных стандартов типа Mifare, EMMARINE, TIRIS… меня часто начал озадачивать такой вопрос – буквально в последний год широкую популярность приобрели разного рода эмуляторы под тэги популярных протоколов и разнообразные копировальщики ключей/брелков. Учитывая большое количество доступных в продаже спец микросхем популярных протоколов RFID и дешевых ридеров, широкого распространения оборудования типа цифровых осцилографов, сниферов и спектроанализаторов, данный вопрос стал для многих разработчиков более актуальным. Тогда я решился сделать для одного из проектов протокол для обмена отличающийся от описанных выше стандартов.

Безусловно данная идея не решает глобальных проблем защищенности новой системы и может быть проанализирована другими разработчиками при наличии оборудования, однако суть в том, что все это не совпадает с существующими стандартами и все железки копировальщиков не позволят по-быстрому скопировать и воссоздать подобный алгоритм. Разумеется подобная система не преподносится тут не как полное решение проблем безопасности, а как опыт адаптации RFID под закрытую систему. Хорошим плюсом в вопросе безопасности среди прочих подобных беспроводных систем является сама технология низкочастотных RFID – она не позволяет считать тэги на большом расстоянии. Пассивные тэги достаточно маломощны и нуждаются для своего питания в достаточно мощном генераторе считывателя, особенности распространения радиоволн на данных частотах также ограничивают пределы работы данной системы. Реальная дальность считывания транспондеров редко превышает 20см для 125 Кгц стандартов типа EmMarine, скажем стандарта EM4001, для других протоколов типа Mifare (13,56Мгц) может быть побольше (1,5 метра для iso15693). Можно добиться большего расстояния считывания для низкочастотных ридеров если увеличить размеры катушки и напряжение питания, соответственно и мощность ридера. Однако такие системы имеют громоздки и как правило их тяжело сделать портативными. Как правило, такие системы реализуются только стационарно – скажем для автомобилей.

Итак, теперь собственно по архитектуре нашей RFID системы. Для экспериментов был выбран контроллер atmel atmega8. Для целей изготовления транспондера это кажется несомненным излишеством. Однако в данном случае решалась первостепенная задача разработки нового интерфейса на готовой отладочной платке с atmega с последующим портированием данного кода на более дешевые контроллеры типа tiny13.

Для транспондера алгоритм работы был построен на основе режима ШИМ генерации при помощи таймера T1 в режиме CTC с прерыванием и сбросом по совпадению с OCR1. Данные для передачи транспондера считываются из EEPROM при включении питания контроллера. Всего транспондер передает 10 байт.

Содержимое EEPROM транспондера можно видеть на рисунке 1. Первый байт 0xE7 является обязательным заголовком пакета, так как его наличие проверяется в первую очередь при разборе пакета считывателем. Первые 8 байт являются содержимым пакета транспондера, последние 2 байта содержат контрольную сумму CRC16 первых восьми байт пакета. Для примера в нашем транспондере были записаны такие данные – пакет 0xE7,0x05,0xE8,0x93,0x43,0x7F,0x20,0xFF и соответственно контрольную сумму 0xF5 0xA8. Для изготовления собственного уникального транспондера нужно кроме первого байта 0xE7 записать семь следующих байт в EEPROM, после чего рассчитать контрольную сумму для первых восьми байт. После этого записать в EEPROM два байта CRC16 в конце пакета. Первый байт оставляем без изменений - 0xE7. При включении транспондера данные этих байт разбиваются по битам и кодируются соответствующей длиной импульса в соответствии со значением регистра OCR. Для передачи используются 2 частоты 2Кгц и 5Кгц для передачи логических “0” и “1”. Кроме того данные разделяются импульсами синхронизации – стартовые метки пакетов.

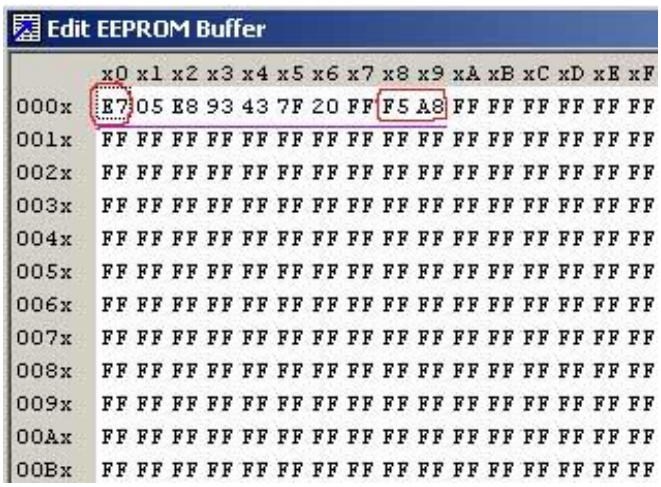

Рис.1 Содержимое пакета транспондера.

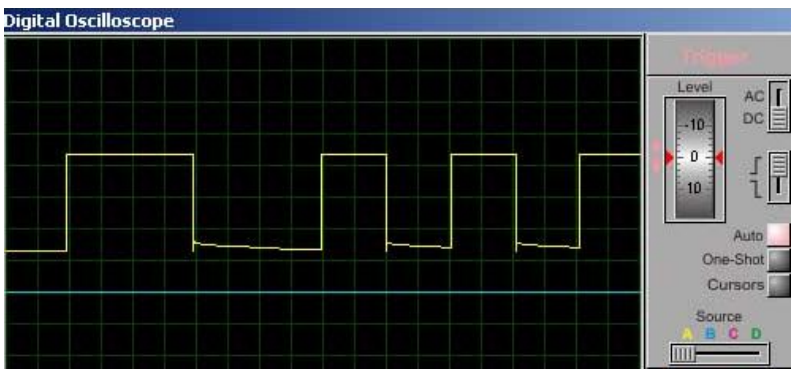

Рис.2 Дамп передачи транспондера на экране виртуального осцилографа.

Схему транспондера можно увидеть на рисунке 3. Частота задающего генератора 8Мгц. Питание контроллера +5В. Можно использовать контроллер mega8 с маркировкой “L” тогда питание можно осуществлять от литиевой батарейки 3в (параметры для такого чипа +2,7…. +3,5). Вместо данного транзистора можно использовать любой другой маломощный NPN транзистор. Катушка транспондера

была намотана на оправке диаметром 50мм проводом 0,22мм и насчитывает 50 витков. На данный момент транспондер сделан активным - с внешним питанием. На следующем этапе планируется сделать пассивный вариант транспондера, что достаточно просто – сделать развязку для питания от данной катушки, добавить диоды моста выпрямителя и стабилизатор.

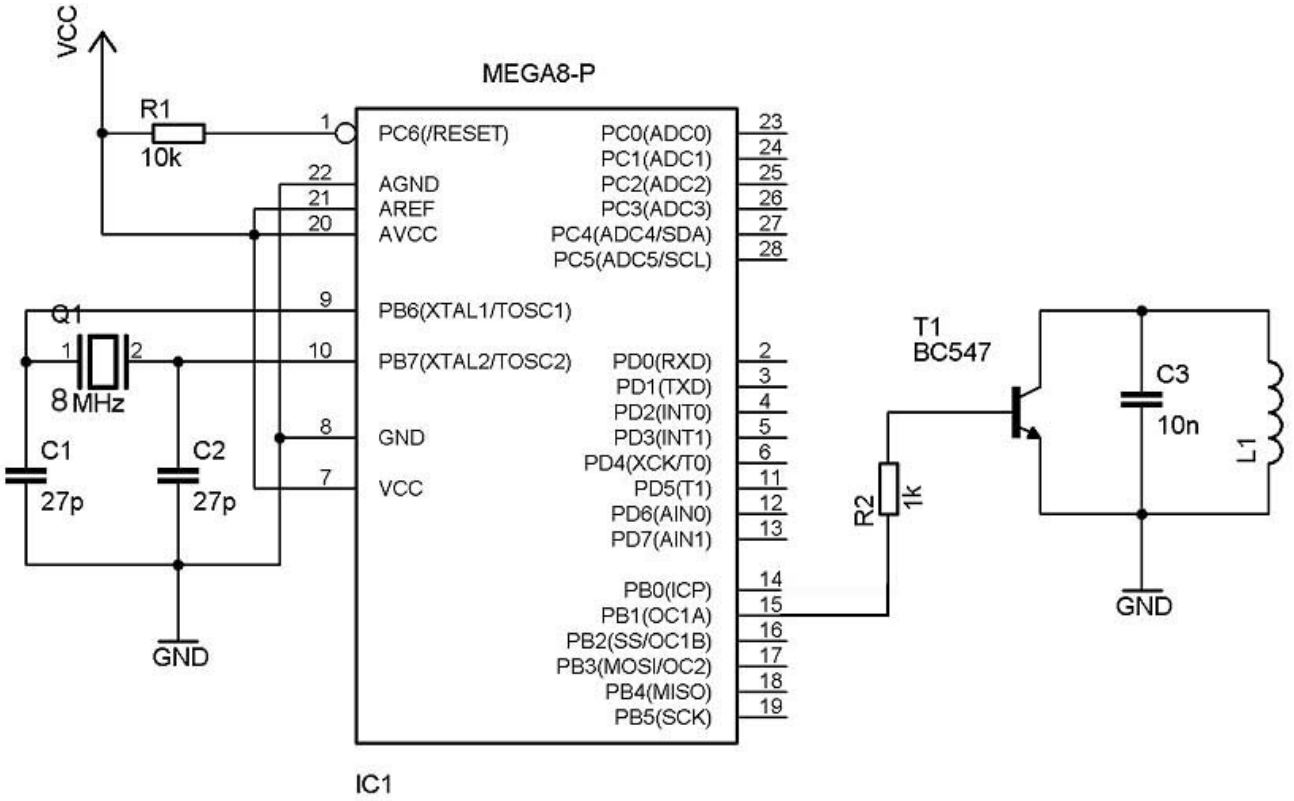

Рис.2 Схема транспондера.

Теперь поговорим о схеме считывателя для данного транспондера. Схема была адаптирована на основе раннее использованного считывателя для карт EMMARINE. Часть схемы с генератором на 74hc4060 можно на данном этапе смело удалять, так как пока мы используем активную метку. Однако эта часть схемы нам понадобится в дальнейшем, когда мы будем делать пассивную метку и нам потребуется получить питание от считывателя. В остальном схема не имеет существенных отличий от схемы считывателя для EMMARINE: пассивный пиковый детектор – фильтр – усилитель – компаратор. Схема имеет максимально возможную простоту и позволяет считывать данные транспондера на расстоянии 10-12см при хорошо настроенных контурах. Можно еще дальше упрощать схему оставив только детектор и фильтр, поставить один транзистор на выходе который будет играть роль компаратора, но я не стал так делать. На выходе мы получаем двоичный сигнал прямоугольной формы в соответствии с кодированными длительностями импульсов передаваемых транспондером. Допустимые отклонения номиналов элементов при котором схема работоспособна 5-10%. Питание контроллера и операционника +5В. Частота кварца задающего генератора

контроллера 12Мгц. Выход компаратора на LM358 подключен к ножке внешнего прерывания контроллера INT0. В программе контроллера настроен вызов прерывания по нарастающему фронту на ножке внешнего прерывания INT0. В обработчике прерывания происходит проверка синхронизирующих импульсов а затем проверка заголовка пакета и запись содержимого в буфер контроллера. Данные считанных пакетов передаются по интерфейсу RS232 на ПК. Для настройки терминалки указываем следующие параметры: скорость 57.6Kb/s, 8 бит данных, 1стоп бит, без контроля четности. При приеме пакета контроллер рассчитывает контрольную сумму принятых байт и передает данные в терминалку (пакет и CRC). В случае совпадения контрольных сумм расчитанной контроллером и принятой в пакете выводится сигнал на ножку PORTB.0 (14) контроллера (LED1 на схеме). Можно подключить в данную точку пищалку со встроенным генератором или светодиод через сопротивление. При считывании корректного ключа контроллер запрещает внешние прерывания и делает задержку 1с перед следующим считыванием. Предусмотрен также режим работы данного считывателя в качестве основы RFID замка. Для этого необходимо в EEPROM контроллера считывателя записать полностью байты дампа транспондера - 10 байт. Данные пишутся в EEPROM считывателя точно также, как в EEPROM транспондера. В данном случае при считывании очередного транспондера и совпадении его с записанным в EEPROM считывателя выводится сигнал на ножку PORTB.1 (15) контроллера (LED2 на схеме). В данную точку можно подключить светодиод через сопротивление или выходной ключ (транзистор) на реле исполнительного устройства. Теперь мы получили RFID замок под конкретный ключ и обычный считыватель в одном флаконе.

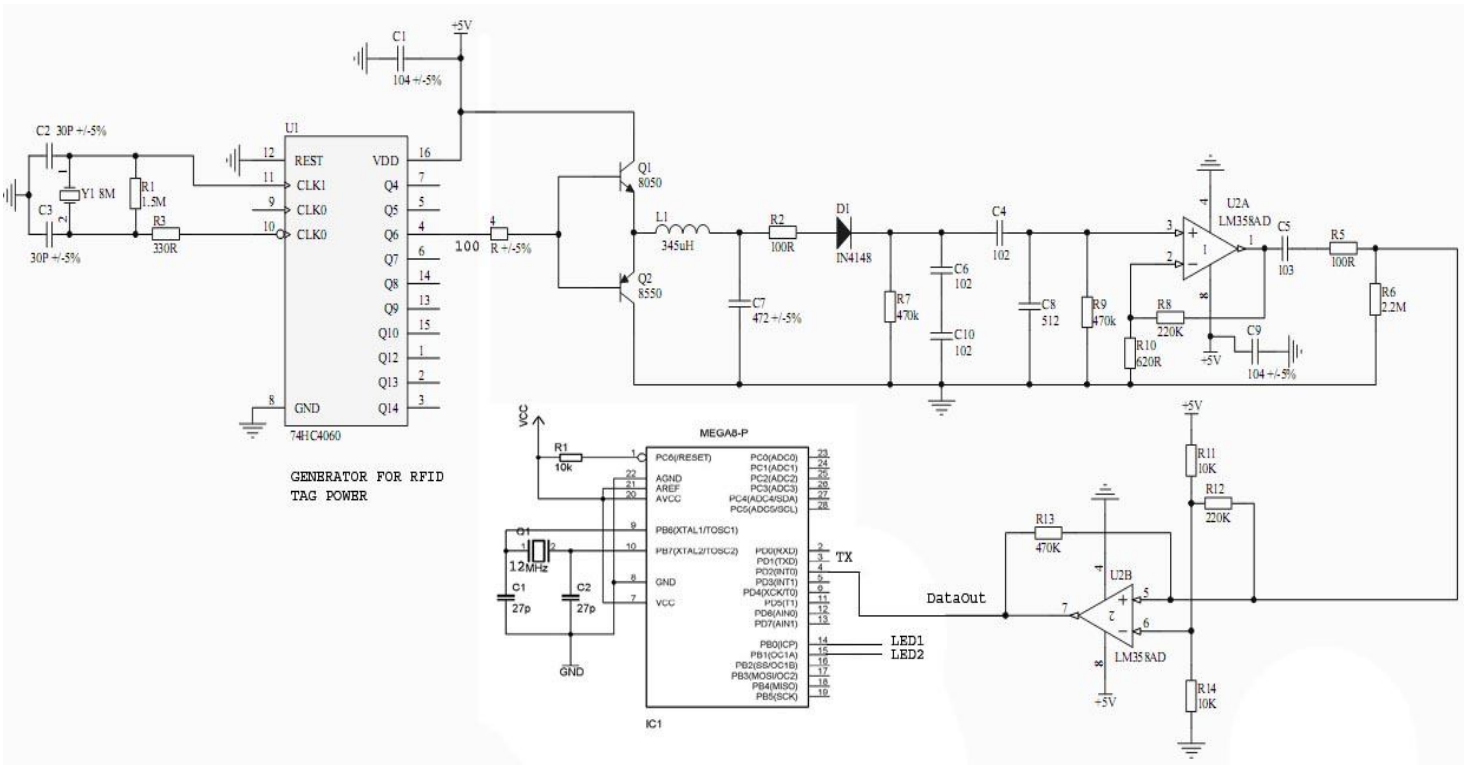

Рис.2 Схема считывателя RFID меток.

Итак, теперь подведем промежуточные итоги. Изготовлен собственный ридер и транспондер под данный считыватель. Мы защитили свое оборудование от посторонних устройств работающих с популярными протоколами RFID. Следующим шагом будет изготовление пассивной метки для нашего считывателя как делают известные производители промышленных транспондеров и портирование кода оборудования на более дешевые модели контроллеров. В архиве к статье прилагаю прошивки для транспондера и считывателя а также соответствующие схемы.

Рубанов К. kostua123@mail.ru