ПРОТОКОЛ ОБМЕНА МЕЖДУ КОНТРОЛЛЕРОМ И ХОСТОМ

1. Общие сведения

Скорость передачи по RS485 – 38400 бит/с.
Формат слова: 8 бит, контроля по четности нет.

Формат пакета

FEND	ADDR	CMD	N	Data1	...	DataN	CRC

FEND: Управляющий код FEND (C0h) является признаком начала пакета. Благодаря стаффингу, этот код больше нигде в потоке данных не встречается, что позволяет в любой ситуации однозначно определять начало пакета.

ADDR: Байт адреса используется для адресации отдельных устройств. На практике распространена ситуация, когда управление осуществляется только одним устройством. В таком случае байт адреса не требуется, и его можно не передавать. Вместо него сразу за кодом FEND передается байт команды CMD. Для того, чтобы можно было однозначно установить, адресом или командой является второй байт пакета, введены некоторые ограничения. Для адресации используется 7 бит, а старший бит, передаваемый вместе с адресом, должен всегда быть установлен:

	D7	D6	D5	D4	D3	D2	D1	D0
ADDR=	1	A6	A5	A4	A3	A2	A1	A0

Иногда возникает необходимость передать какую-то команду или данные сразу всем устройствам. Для этого предусмотрен коллективный вызов (broadcast), который осуществляется путем передачи нулевого адреса (учитывая единичный старший бит, в этом случае передаваемый байт равен 80h). Нужно отметить, что передача в пакете нулевого адреса полностью аналогична передаче пакета без адреса. Поэтому при реализации протокола можно автоматически исключать нулевой адрес из пакета. Учитывая разрядность адреса и один зарезервированный адрес для коллективного вызова, максимальное количество адресуемых устройств составляет 127.
Если возникает необходимость передать значение адреса 40h или 5Bh (передаваемый байт в этом случае будет равен C0h или DBh), то производится стаффинг, т.е. передача ESC-последовательности. Поэтому следует учитывать, что устройства с такими адресами требуют большей на один байт длины пакета. Это может быть заметно в тех случаях, когда используются короткие пакеты. В таких случаях следует избегать назначения устройствам названных адресов.

CMD: Байт команды всегда должен иметь нулевой старший бит:

	D7	D6	D5	D4	D3	D2	D1	D0
CMD=	0	C6	C5	C4	C3	C2	C1	C0

Таким образом, код команды занимает 7 бит, что позволяет передавать до 128 различных команд. Коды команд выбираются произвольно в зависимости от нужд приложения. Рекомендуется использовать несколько стандартных кодов команд:

Протокол обмена с M6

Стандартные коды команд протокола.

Код	Название	Описание команды
00h	C_Nop	Нет операции
01h	C_Err	Передача кода ошибки
02h	C_Echo	Запрос возврата переданного пакета
03h	C_Info	Запрос информации об устройстве

Коды остальных команд выбираются в зависимости от нужд приложения. Команды обычно имеют несколько параметров, которые передаются далее в виде пакета данных. Поскольку код команды всегда имеет нулевой старший бит, этот код никогда не совпадает с управляющими кодами. Поэтому при передаче команды стаффинг никогда не производится.

N: Байт количества данных имеет значение, равное количеству передаваемых байт данных:

	D7	**D6**	**D5**	**D4**	**D3**	**D2**	**D1**	**D0**
N=	**N7**	**N6**	**N5**	**N4**	**N3**	**N2**	**N1**	**N0**

Таким образом, код количества данных занимает 8 бит, в результате один пакет может содержать до 255 байт данных. Значение N не учитывает служебные байты пакета FEND, ADDR, CMD, N и CRC. В результате стаффинга фактическая длина пакета может возрасти. Значение N не учитывает этот факт и отражает количество полезных байт данных (т.е. значение N всегда таково, как будто стаффинг не осуществляется). Если передаваемая команда не имеет параметров, то передается N = 00h и байты данных опускаются.
Если возникает необходимость передать значение N, равное C0h или DBh, то производится стаффинг, т.е. передача ESC-последовательности (см. таблицу 2). Однако при таких больших значениях N длина пакета столь велика, что его удлинение еще на один байт практически незаметно.

Data1...DataN: Байты данных, количество которых определяется значением N. При N = 00h байты данных отсутствуют. Байты данных могут иметь любое значение, кроме FEND (C0h) и FESC (DBh). Если возникает необходимость передать одно из этих значений, то производится стаффинг, т.е. передача ESC-последовательности (см. таблицу 2), состоящей из управляющего кода FESC и кода TFEND (TFESC).

CRC: Байт контрольной суммы CRC-8. Может отсутствовать в **некоторых** реализациях протокола. Контрольная сумма CRC-8 рассчитывается **перед** операцией стаффинга для всего пакета, начиная с байта FEND и заканчивая последним байтом данных. Если в пакете передается адрес, то при вычислении контрольной суммы используется его истинное значение, т.е. единичный старший бит не учитывается. Для расчета контрольной суммы используется полином CRC = X8 + X5 + X4 + 1. Значение CRC перед вычислением инициализируется адресом контроллера. При передаче значения байта контрольной суммы C0h и DBh заменяются ESC-последовательностями.

Байт данных	Передаваемая последовательность
C0h	DBh, DCh
DBh	DBh, DDh

2. Команды	
Отправитель	**Хост**
Приемник	**Контроллер**

Коды команд лежат в диапазоне: 00h – 7Fh (0 - 127).

Код адреса, передаваемый по сети, лежит в диапазоне: 80h – FFh. То есть в соответствии с WAKE старший бит всегда равен 1. При декодировании старший бит отбрасывается и получается адрес от 0 до 127. **0 или 0x80h зарезервирован для широковещательных команд.**
При передаче широковещательных команд допускается после FEND сразу же передавать код команды. Таким образом, если необходимо однозначно указать нулевой адрес, код адреса должен быть установлен 80h. Тогда следующий принятый байт будет воспринят как код команды. Числа ниже 80h принимаются контроллером как код команды в пакете с нулевым адресом. То есть если пришел пакет с полем адреса равным нулю, контроллер считает, что пришла команда по нулевому адресу равная нулю. По спецификации WAKE это пустая операция.

Пример: принятый адрес - 0xC1. Убиваем старший бит: ADDR = C1h – 80h = 41h (65 dec.). Или ADDR = C1h & 7Fh = 41h (65 dec.).

Максимальный размер блока данных (N) 255 байт. Это без учета FEND, ADDR, N, CRC. Таким образом буфер **передаваемых** данных должен иметь размер не менее 259 байт. С учетом байтстаффинга рекомендуется увеличить размер буфера до 512 байт.

```
//**********************************************************
//Команды
//**********************************************************
//Стандартные коды команд протокола
0x00    //нет операции (никогда не используется)
0x01    //передача кода ошибки (передается хосту, если пакет
        //принят с ошибкой, например ошибка CRC
0x02    //запрос возврата переданного пакета (проверка связи)
0x03    //запрос информации об устройстве
0x04    //повторить последний переданный пакет
```

2.1 Команды общего назначения [0Xh]	
Отправитель	**Хост**
Приемник	**Оборудование**

2.1.1 Пустая операция [00h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Данная команда не используется в системе. Контроллер ее игнорирует

2.1.2 Передача результата выполнения команды (кода ошибки) [01h]	
Отправитель	**Оборудование**
Приемник	**Хост**

Оборудование шлет пакет вида:

FEND	**ADDR**	**01h**	**1**	**ERR_CODE**	**CRC**

Протокол обмена с М6
ERR_CODE – результат выполнения команды. Его значения могут быть:

Код	Описание	Примечание
0	Нормальное выполнение команды	
1	Пакет принят с некорректной CRC	
2	Неправильные параметры команды	
3	Пакет принят с некорректной ESC послед-ю	
4	Устройство не готово	
5	Устройство неисправно	

Данный пакет возвращается контроллером хосту в качестве подтверждения выполнения команды, а также в случае некорректности содержимого пакета или невозможности выполнения команды.

2.1.3 Запрос возврата переданного пакета (проверка связи) [02h]	
Отправитель **Приемник**	**Хост** **Оборудование**

Хост шлет пакет вида:

FEND	ADDR	02h	N	Data1	...	DataN	CRC

Контроллер возвращает:

FEND	ADDR	02h	N	Data1	...	DataN	CRC

В качестве Data1 – DataN могут быть любые произвольные данные.

2.1.4 Запрос информации об устройстве [03h]	
Отправитель **Приемник**	**Хост** **Оборудование**

Хост шлет пакет вида:

FEND	ADDR	03h	0h	CRC

Контроллер возвращает:

FEND	ADDR	03h	N	Data1	...	DataN	CRC

-1 байт – тип устройства
10h – М6.

В коде заводятся три константы DEVICE_TYPE, DEVICE_VERSION, DEVICE_SUBVERSION, которые будут иметь соответствующее значение и которые будут по запросу передаваться.

-2 байт – версия

-3 байт – субверсия

2.1.5 Запрос повтора последнего переданного пакета [04h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	04h	0h	CRC

Контроллер возвращает:

Последний переданный пакет.

2.1.6 Запрос передачи состояния контроллера [05h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	05h	0h	CRC

Контроллер возвращает:

FEND	ADDR	05h	N	Data1	...	DataN	CRC

-1 байт –флаги состояния системы

0 бит – Признак рестарта. 1 – первый запрос после рестарта. 0 – все остальные.
Сбрасывается после считывания состояния.
1 бит – Резерв.
2 бит – Резерв.
3 бит – Резерв.
4 бит – Резерв.
5 бит – Резерв.
6 бит – Резерв.
7 бит – Резерв.

2.1.7 Рестарт контроллера [08h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	08h	0	CRC

Контроллер возвращает:

Код ошибки. После перезагрузки можно запросить состояние и по соответствующему биту убедиться, что контроллер перезапустился.

2.1.8 Команды прямого доступа к памяти [09h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Протокол обмена с М6

Хост шлет пакет вида:

FEND	ADDR	09h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров:

- 1 байт – команда.

Команда	Описание	Примечание
01h	Читать содержимое EEPROM	
02h	Записать данные EEPROM	

- 2(LSB), 3, 4(MSB) байт – начальный адрес блока считываемых/записываемых данных.

Значение адреса передается младшим байтом вперед.

- 5 байт – длина данных.

Для команды записи – это длина записываемых данных, которые предаются в данном пакете. Для команды чтения – это длина данных, которые должны быть переданы из контроллера. Блок передаваемых данных максимально может быть равен 250 байт: 255 – 5 байт.

-6 байт…250 байт. – данные.

Контроллер возвращает:

Возвращается код ошибки (п.2.1.2) с соответствующим значением или пакет с результатом.
Если была команда чтения и данные успешно считаны в буфер:

FEND	ADDR	09h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров результата выполнения команды:

-1 байт…250 байт. – данные.

Максимально возможно передать 250 байт.

Пример:
ПО считывает блок данных с адрес 0x000000 длиной 34 байта:
C0 81 09 05 01 00 00 00 22 E5
Контроллер возвращет:
C0 81 09 22 12 34 01 02 01 02 00 00 1F 00 4C 00 5E B6 65 2F 4D 5B 9D 3A B8 18 7B DB DD 28 D1 00 03 02 0A 01 00 00 00 6C

2.1.9 Управление контроллером [10h]	
Отправитель **Приемник**	**Хост** **Оборудование**

Хост шлет пакет вида:

FEND	ADDR	10h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров:

- 1 байт – команда.

Команда	Описание	Примечание
01h	Разблокировать замок	
02h	Разблокировать замок надолго	
03h	Заблокировать замок	
04h	Заблокировать замок надолго	

Протокол обмена с M6
Контроллер возвращает:

Возвращается код ошибки с соответствующим значением или пакет с результатом.

FEND	ADDR	10h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров результата выполнения команды:
- 1 байт – результат.
0x01 – нет ошибки.
0x02 – неверные параметры команды.

2.2 Команды Mifare [4Xh]	
Отправитель	**Хост**
Приемник	**Считыватель**

2.2.1 Команда получения серийного номера карты [40h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	40h	0	CRC

Контроллер возвращает:

FEND	ADDR	40h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров результата выполнения команды:
- 1 байт – результат выполнения
0 - ошибка
1 – успешно
- 2,3 байт – ATQA
- 4 байт – SAQ
- 5 байт RFAL TYPE
- 6 байт длина UID
- 7..16 байт - UID

2.2.4 Команда доступа к памяти карты Mifare Plus [43h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	43h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров:
- 1 байт – команда.

Команда	Описание	Примечание
01h	**Читать содержимое памяти карты**	
02h	**Записать данные в память карты**	
03h	**Записать ключ**	

-2 байт – тип ключа.
0 - Ключ А

Протокол обмена с М6
1 - Ключ B

- 3 байт – сектор.
- 4 байт – блок.

- 5(LSB) – 20(MSB) байт – AES ключ.

-21 байт…36 байт. – данные.

Контроллер возвращает:

FEND	ADDR	42h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров результата выполнения команды:
- 1 байт – код результата выполнения команды.

Команда	Описание	Примечание
01h	**Успешно выполнено**	
02h	**Карта отсутствует в поле**	
03h	**Ошибка аутентификации**	
04h	**Ошибка верификации данных**	

-2 байт…17 байт. – данные.
Максимально возможно передать 16 байт.

2.2.5 Команда Perso Mifare Plus [44h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	44h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров:
- 1 байт – команда.

Команда	Описание	Примечание
01h	**Запись ключей**	
02h	**Переключение SL3**	
03h	**Переключение SL0 -> SL3**	

- 2-17 байт – KeyA
- 18-23 байт – KeyB
- 24-39 байт – CardMasterKey
- 40-55 байт – CardConfKey
- 56-71 байт – Lewel3SwitchKey
- 72-87 байт – SL1CardAuthKey

2.2.6 Работа с картой объекта [45h]	
Отправитель	**Хост**
Приемник	**Оборудование**

Хост шлет пакет вида:

FEND	ADDR	45h	N	Data1	...	DataN	CRC

Протокол обмена с М6
Где в качестве Data передается блок параметров:
- 1 байт – команда.

Команда	Описание	Примечание
01h	**Чтение записи из списка карт объекта**	
02h	**Включение режима добавления карт объекта в список карт объекта**	
04h	**Включение режима создания карт объекта**	
06h	**Удаление одной записи из списка карт объекта**	
08h	**Включение режима создания карт прохода**	
09h	**Очистка карты прохода**	
0Ah	**Очистка карты объекта**	
0Bh	**Включение режима переключения SL0->SL3**	

- 2 – 5 байт – пароль карты объекта
- 6 – 7 байт – версия карты объекта
- 8 байт – наследуемый тип карты прохода
- 9 байт – номер в списке карт объекта

Контроллер возвращает:

FEND	ADDR	45h	N	Data1	...	DataN	CRC

Где в качестве Data передается блок параметров результата выполнения команды:
- 1 байт – код результата выполнения команды.

Команда	Описание	Примечание
01h	**Успешно выполнено**	
02h	**Карта отсутствует в поле**	
03h	**Ошибка аутентификации**	
04h	**Ошибка верификации данных**	

- 2 байт – команда, в ответ на которую передается данный пакет с ответом.
-3 байт…21 байт. – данные.