

ModBus RTU

1. Режим UART – 1 старт – 8 данные – 1 стоп, или 2 стоп, без контроля четности. Емкость буфера – 40 байт, т.е. длина пакета от ModBus-адреса до контрольной суммы включительно не должна превышать 40 байт.

2. Структура пакета ModBus

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1–T2–T3–T4	8 BITS	8 BITS	$n \times 8$ BITS	16 BITS	T1–T2–T3–T4

START, END – Задержка между пакетами, не менее 3,5 знаков. Здесь Знак – время передачи одного символа на выбранной скорости (т.е. $(1+8+1)/(\text{BaudRate})$).

ADDRESS – Адрес устройства Modbus, 1..247;

FUNCTION – Функция устройства ModBus. В устройстве используются:

- 0x03 – Чтение регистра(ов) типа HOLDING (регистр - чтение/запись);
- 0x04 – Чтение регистра(ов) типа INPUT (регистр – только чтение);
- 0x06 – Запись одного регистра типа HOLDING;
- 0x10 – Запись регистров типа HOLDING (последовательно расположенных);
- 0x11 – Чтение строки идентификации («о приборе»).

DATA – Адрес регистра, далее:

для функций 0x03, 0x04, 0x06 – количество БАЙТ данных;

для функции 0x10 – количество записываемых регистров ModBus, и далее

количество БАЙТ данных;

далее – собственно, сами данные.

Все данные – 16ти разрядные, 8ми разрядные типа char дополняются старшим байтом с нулевым значением. Данные формата float (4 байта) разбиваются на пару 16ти разрядных значений, старшее передается первым. Исходя из того, что числа с плавающей точкой передаются через 2 Modbus регистра, запись таких значений производится только посредством функции 0x10.

CRC CHECK – Контрольная сумма по стандарту CRC-16-ANSI (не CRC-16-CCITT!), младший байт первым (LSB, MSB). Более подробно: MB Protocol.pdf, Appendix C LRC/CRC Generation.

Все значения (адрес, регистр, количество байт, данные) передаются старшим байтом вперед. Исключение составляет только контрольная сумма – младший байт идет первым.

Важно!

Задержка между пакетами – не менее 3,5 знаков (символа).

Задержка между байтами в пакете не более 1,5 знака (символа).

Если в пакете будет обнаружена задержка более 1,5 знаков – следующие данные воспринимаются как новый пакет

(поэтому нельзя с терминалки выводить побайтно, выводить нужно весь пакет сразу).

Структура пакета ответа проще, поэтому здесь не приводится.

При ошибке в пакете ответа за ModBus адресом следует код, соответствующий функции в запросе со старшим битом установленным в 1 (например, запрашивали функцию 0x04, ответ ошибки будет 0x84). Далее выводится код ошибки, соответствующий:

0x02 – при попытке обращения к несуществующему регистру;

0x03 – при попытке ввода параметра вне допустимого диапазона.

3. Структура регистров

Регистры типа INPUT (только чтение, функция ModBus 0x04):

Адрес Тип Значение

0000 u16 Измеренное значение напряжения, в кодах, 0..65535

0001 u16 Измеренное значение тока, в кодах, 0..65535

0002 u16 Внешние входы MSB - не используется, 0x00.

0 – нет, 1 – да :

LSB.7 - Перегрузка по напряжению;

LSB.6 - Перегрузка по току;

LSB.5 - Перегрев;

LSB.4 - не используется;

LSB.3 - не используется;

LSB.2 - Ждущий режим;

LSB.1 - Режим ограничения по напряжению;

LSB.0 - Режим ограничения по току;

0003 u16 Не используется, возвращает 0x0000;

0004 float Не используется, возвращает 1.037892348

(0005 – пропущенный формальный адрес для младших 2х байт числа с плавающей запятой)

(Старший 16ти разрядный регистр будет прочитан как 0x3F84, младший – 0xD9A8).

Регистры типа Holding (чтение/запись, функции чтения ModBus 0x03 или 0x10)

Адрес Тип Значение

0000 u16 Адрес ModBus, 1..247, по умолчанию адрес = 1.

0001 u16 Скорость UART, индексом 0..5, соответственно:

0: 4800,

1: 9600,

2: 19200,

3: 38400,

4: 57600,

5: 115200.

По умолчанию установлена скорость 9600, т.е. индекс = 1.

0002 u16 Задержка RTS, 0..255 – задержка управлением направлением потока при использовании интерфейса RS485, функция не реализована ввиду отсутствия необходимости.

Управление направлением потока происходит в автоматическом режиме, без задержек.

Устройство находится постоянно в режиме приема, переходя в режим передачи на время ответа.

0003 u08 Тип PSU Индекс 0..11, соответственно:

Индекс	Верхний предел напряжения, В	Верхний предел тока, А
0	27,5	30,0
1	55,0	15,0
2	60,0	30,0
3	30,0	90,0
4	110	7,5
6	220	3,8
7	330	2,5
8	440	1,9
9	550	1,5
10	660	1,2
11	установленное значение, до 999,9	установленное значение, до 999,9

По умолчанию установлен тип 27,5В/30,0А, т.е. индекс = 0. Для типа с индексом 11 верхние пределы напряжения и тока устанавливаются в регистрах 0x000F и 0x0010 соответственно.

0004 u16 Значение генератора ШИМ напряжения, 0...0x03FF. Управление значением выходного напряжения, соответственно от 0 до верхнего предела напряжения. Непосредственно на выходе самого модуля управления – 0..5В.

0005 u16 Значение генератора ШИМ тока, 0..0x03FF. Аналогично, тока.

0006 float Калибровочное значение аддитивной поправки канала измерения напряжения. По умолчанию = 0.0. Пределы определяются диапазоном значений типа переменной (float). При передаче значения, как было сказано выше, первым передается старший байт, последним – младший.

(0007 – пропущенный формальный адрес для младших 2х байт числа с плавающей запятой)

0008 float Калибровочное значение мультипликативной поправки канала измерения напр. По умолчанию = 1.0.

(0009 – пропущенный формальный адрес для младших 2х байт числа с плавающей запятой)

000A float Калибровочное значение аддитивной поправки канала измерения тока. По умолчанию = 0.0.

(000B – пропущенный формальный адрес для младших 2х байт числа с плавающей запятой)

000C float Калибровочное значение мультипликативной поправки канала измерения тока. По умолчанию = 1.0.

(000D – пропущенный формальный адрес для младших 2х байт числа с плавающей запятой)

Калибровочные значения влияют только на отображаемые на дисплее результаты измерений и не влияют на значения регистров измеренных значений напряжения и тока (регистры INPUT 0x0000 и 0x0001 соответственно).

Отображаемые значения напряжения и тока рассчитываются по следующим выражениям:

$$\text{Отображаемая величина} = \text{аддитивная поправка} + \\ + (\text{приведенное измеренное значение} * \text{мультипликативная поправка} * \text{верхний предел величины});$$

где:

приведенное измеренное значение – измеренное значение, приведенное к единице, т.е.

применительно к АЦП – $D_{\text{ADC}}/D_{\text{FSR}}$;

верхний предел величины – в соответствии с таблицей Тип PSU

000E u16 Ждущий режим, 0 или 1. 0 – рабочий режим, 1 – режим ожидания. В режиме ожидания выходные сигналы остаются активными, на дисплей выводится надпись «STANDBY», однако результаты измерений не отображаются.

000F u16 Верхний предел напряжения для настраиваемого типа (см. Тип PSU), в десятых долях вольт, 0...9999;

0010 u16 Верхний предел тока для настраиваемого типа, (см. Тип PSU), в десятых долях ампер, 0...9999;

Соответственно устанавливаемые максимальные пределы составляют 999,9В и 999,9А.

4. Ответ запроса по функции ModBus 0x11

Структура запроса:

Адрес ModBus – Функция 0x11 – CRC-16

Структура ответа:

Адрес ModBus – Функция 0x11 – Количество байт – Строка идентификации – CRC-16

Строка идентификации для данного модуля: «EL PSU Control (c) 2010 Elim Ltd.»

По опыту работы наиболее типичными ошибками при работе с ModBus являются:

а) Несоблюдение установленных тайм-аутов (1,5 знака и 3,5 знака)

б) Неправильная последовательность байт (MSB, LSB)

в) Неверный полином для подсчета CRC-16, например довольно широко распространенный в модемах CRC-16-CCITT.