Описание протокола Modbus RTU

Modbus — коммуникационный протокол, основан на архитектуре ведущий-ведомый (master-slave). Использует для передачи данных интерфейсы RS-485, RS-422, RS-232, а также Ethernet сети TCP/IP (протокол Modbus TCP).

Сообщение Modbus RTU состоит из адреса устройства SlaveID, кода функции, специальных данных в зависимости от кода функции и CRC контрольной суммы.

SlaveID	Код функции	Специальные данные	CRC

Если отбросить SlaveID адрес и CRC контрольную сумму, то получится PDU, Protocol Data Unit.

SlaveID – это адрес устройства, может принимать значение от 0 до 247, адреса с 248 до 255 зарезервированы.

Данные в модуле хранятся в 4 таблицах.

Две таблицы доступны только для чтения и две для чтения-записи.

В каждой таблице помещается 9999 значений.

Номер регистра	Адрес регистра HEX	Тип	Название	Тип
1-9999	0000 до 270E	Чтение-запись	Discrete Output Coils	DO
10001-19999	0000 до 270E	Чтение	Discrete Input Contacts	DI
30001-39999	0000 до 270E	Чтение	Analog Input Registers	AI
40001-49999	0000 до 270E	Чтение-запись	Analog Output Holding Registers	AO

В сообщении Modbus используется адрес регистра.

Например, **первый** регистр AO Holding Register, имеет **номер** 40001, но его **адрес** равен 0000.

Разница между этими двумя величинами есть смещение offset.

Каждая таблица имеет свое смещение, соответственно: 1, 10001, 30001 и 40001.

Ниже приведен пример запроса Modbus RTU для получения значения AO аналогового выхода (holding registers) из регистров от #40108 до 40110 с адресом устройства 17.

11 03 006B 0003 7687

11	Адрес устройства SlaveID (17 = **11** hex)
03	Функциональный код Function Code (читаем Analog Output Holding Registers)
006B	Адрес первого регистра (40108-40001 = 107 =**6B** hex)
0003	Количество требуемых регистров (чтение 3-х регистров с 40108 по 40110)
7687	Контрольная сумма CRC

В ответе от Modbus RTU Slave устройства мы получим:

11 03 06 AE41 5652 4340 49AD

Где:

11	**Адрес устройства** (17 = 11 hex)	SlaveID
03	**Функциональный код**	Function Code
06	**Количество байт далее** (6 байтов идут следом)	Byte Count
AE	**Значение старшего разряда регистра** (AE hex)	Register value Hi (AO0)

41	**Значение младшего разряда регистра** (41 hex)	Register value Lo (AO0)
56	**Значение старшего разряда регистра** (56 hex)	Register value Hi (AO1)
52	**Значение младшего разряда регистра** (52 hex)	Register value Lo (AO1)
43	**Значение старшего разряда регистра** (43 hex)	Register value Hi (AO2)
40	**Значение младшего разряда регистра** (40 hex)	Register value Lo (AO2)
49	**Контрольная сумма**	CRC value Lo
AD	**Контрольная сумма**	CRC value Hi

Регистр аналогового выхода AO0 имеет значение AE 41 HEX или 44609 в десятичной системе.
Регистр аналогового выхода AO1 имеет значение 56 52 HEX или 22098 в десятичной системе.
Регистр аналогового выхода AO2 имеет значение 43 40 HEX или 17216 в десятичной системе.
Значение AE 41 HEX - это 16 бит 1010 1110 0100 0001, может принимать различное значение, в зависимости от типа представления.
Значение регистра 40108 при комбинации с регистром 40109 дает 32 бит значение.
Пример представления.

Тип представления	Диапазон значений	Пример в HEX	Будет в десятичной форме
16-bit unsigned integer	0 до 65535	AE41	44,609
16-bit signed integer	-32768 до 32767	AE41	-20,927
two character ASCII string	2 знака	AE41	® A
discrete on/off value	0 и 1	0001	0001
32-bit unsigned integer	0 до 4,294,967,295	AE41 5652	2,923,517,522
32-bit signed integer	-2,147,483,648 до 2,147,483,647	AE41 5652	-1,371,449,774
32-bit single precision IEEE floating point number	1,2·10−38 до 3,4×10+38	AE41 5652	-4.395978 E-11
four character ASCII string	4 знака	AE41 5652	® A V R

Какие бывают команды Modbus RTU?
Приведем таблицу с кодами функций чтения и записи регистров Modbus RTU.

Код функции	Что делает функция		Тип значения	Тип доступа
01 (0x01)	Чтение DO	Read Coil Status	Дискретное	Чтение
02 (0x02)	Чтение DI	Read Input Status	Дискретное	Чтение
03 (0x03)	Чтение AO	Read Holding Registers	16 битное	Чтение
04 (0x04)	Чтение AI	Read Input Registers	16 битное	Чтение
05 (0x05)	Запись одного DO	Force Single Coil	Дискретное	Запись
06 (0x06)	Запись одного AO	Preset Single Register	16 битное	Запись

15 (0x0F)	Запись нескольких DO	Force Multiple Coils	Дискретное	Запись
16 (0x10)	Запись нескольких AO	Preset Multiple Registers	16 битное	Запись

Как послать команду Modbus RTU на чтение дискретного вывода? Команда 0x01

Эта команда используется для чтения значений дискретных выходов DO.

В запросе PDU задается начальный адрес первого регистра DO и последующее количество необходимых значений DO. В PDU значения DO адресуются, начиная с нуля.

Значения DO в ответе находятся в одном байте и соответствуют значению битов.

Значения битов определяются как 1 = ON и 0 = OFF.

Младший бит первого байта данных содержит значение DO адрес которого указывался в запросе. Остальные значения DO следуют по нарастающей к старшему значению байта. Т.е. справа на лево.

Если запрашивалось меньше восьми значений DO, то оставшиеся биты в ответе будут заполнены нулями (в направлении от младшего к старшему байту). Поле Byte Count **Количество байт далее** указывает количество полных байтов данных в ответе.

Пример запроса DO с 20 по 56 для SlaveID адреса устройства 17. Адрес первого регистра будет 0013 hex = 19, т.к. счет ведется с 0 адреса (0014 hex = 20, -1 смещение нуля = получаем 0013 hex = 19).

Байт	Запрос	Байт	Ответ
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
01	Функциональный код	01	Функциональный код
00	Адрес первого регистра Hi байт	05	Количество байт далее
13	Адрес первого регистра Lo байт	CD	Значение регистра DO 27-20 (1100 1101)
00	Количество регистров Hi байт	6B	Значение регистра DO 35-28 (0110 1011)
25	Количество регистров Lo байт	B2	Значение регистра DO 43-36 (1011 0010)
0E	Контрольная сумма CRC	0E	Значение регистра DO 51-44 (0000 1110)
84	Контрольная сумма CRC	1B	Значение регистра DO 56-52 (0001 1011)
		45	Контрольная сумма CRC
		E6	Контрольная сумма CRC

Состояния выходов DO 27-20 показаны как значения байта CD hex, или в двоичной системе 1100 1101.

В регистре DO 56-52 5 битов справа были запрошены, а остальные биты заполнены нулями до полного байта (**000**1 1011).

Каналы	-	-	-	DO 56	DO 55	DO 54	DO 53	DO 52
Биты	0	0	0	1	1	0	1	1
Hex	1B							

Как послать команду Modbus RTU на чтение дискретного ввода? Команда 0x02

Эта команда используется для чтения значений дискретных входов DI.

Пример запроса DI с регистров от #10197 до 10218 для SlaveID адреса устройства 17. Адрес первого регистра будет 00C4 hex = 196, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	Ответ
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
02	Функциональный код	02	Функциональный код
00	Адрес первого регистра Hi байт	03	Количество байт далее
C4	Адрес первого регистра Lo байт	AC	Значение регистра DI 10204-10197 (1010 1100)
00	Количество регистров Hi байт	DB	Значение регистра DI 10212-10205 (1101 1011)
16	Количество регистров Lo байт	35	Значение регистра DI 10218-10213 (0011 0101)
BA	Контрольная сумма CRC	20	Контрольная сумма CRC
A9	Контрольная сумма CRC	18	Контрольная сумма CRC

Как послать команду Modbus RTU на чтение аналогового вывода? Команда 0x03

Эта команда используется для чтения значений аналоговых выходов AO.

Пример запроса AO с регистров от #40108 до 40110 для SlaveID адреса устройства 17. Адрес первого регистра будет 006B hex = 107, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	Ответ
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
03	Функциональный код	03	Функциональный код
00	Адрес первого регистра Hi байт	06	Количество байт далее
6B	Адрес первого регистра Lo байт	AE	Значение регистра Hi #40108
00	Количество регистров Hi байт	41	Значение регистра Lo #40108
03	Количество регистров Lo байт	56	Значение регистра Hi #40109
76	Контрольная сумма CRC	52	Значение регистра Lo #40109
87	Контрольная сумма CRC	43	Значение регистра Hi #40110
		40	Значение регистра Lo #40110
		49	Контрольная сумма CRC
		AD	Контрольная сумма CRC

Как послать команду Modbus RTU на чтение аналогового ввода? Команда 0x04
Эта команда используется для чтения значений аналоговых входов AI.
Пример запроса AI с регистра #30009 для SlaveID адреса устройства 17. Адрес первого регистра будет 0008 hex = 8, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	Ответ
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
04	Функциональный код	04	Функциональный код
00	Адрес первого регистра Hi байт	02	Количество байт далее
08	Адрес первого регистра Lo байт	00	Значение регистра Hi #30009
00	Количество регистров Hi байт	0A	Значение регистра Lo #30009
01	Количество регистров Lo байт	F8	Контрольная сумма CRC
B2	Контрольная сумма CRC	F4	Контрольная сумма CRC
98	Контрольная сумма CRC		

Как послать команду Modbus RTU на запись дискретного вывода? Команда 0x05
Эта команда используется для записи одного значения дискретного выхода DO.
Значение FF 00 hex устанавливает выход в значение включен ON.
Значение 00 00 hex устанавливает выход в значение выключен OFF.
Все остальные значения недопустимы и не будут влиять значение на выходе.
Нормальный ответ на такой запрос - это эхо (повтор запроса в ответе), возвращается после того, как состояние DO было изменено.
Пример записи в DO с регистром #173 для SlaveID адреса устройства 17. Адрес регистра будет 00AC hex = 172, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	Ответ
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
05	Функциональный код	05	Функциональный код
00	Адрес первого регистра Hi байт	00	Адрес первого регистра Hi байт
AC	Адрес первого регистра Lo байт	AC	Адрес первого регистра Lo байт
FF	Значение Hi байт	FF	Значение Hi байт
00	Значение Lo байт	00	Значение Lo байт
4E	Контрольная сумма CRC	4E	Контрольная сумма CRC
8B	Контрольная сумма CRC	8B	Контрольная сумма CRC

Состояние выхода DO173 поменялось с выключен OFF на включен ON.

Как послать команду Modbus RTU на запись аналогового вывода? Команда 0x06
Эта команда используется для записи одного значения аналогового выхода AO.

Пример записи в AO с регистром #40002 для SlaveID адреса устройства 17. Адрес первого регистра будет 0001 hex = 1, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	Отв
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
06	Функциональный код	06	Функциональный ко
00	Адрес первого регистра Hi байт	00	Адрес первого реги
01	Адрес первого регистра Lo байт	01	Адрес первого реги
00	Значение Hi байт	00	Значение Hi байт
03	Значение Lo байт	03	Значение Lo байт
9A	Контрольная сумма CRC	9A	Контрольная сумма
9B	Контрольная сумма CRC	9B	Контрольная сумма

Как послать команду Modbus RTU на запись нескольких дискретных выводов? Команда 0x0F
Эта команда используется для записи нескольких значений дискретного выхода DO.
Пример записи в несколько DO с регистрами от #20 до #29 для SlaveID адреса устройства 17. Адрес регистра будет 0013 hex = 19, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	От
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
0F	Функциональный код	0F	Функциональный
00	Адрес первого регистра Hi байт	00	Адрес первого рег
13	Адрес первого регистра Lo байт	13	Адрес первого рег
00	Количество регистров Hi байт	00	Кол-во записанны
0A	Количество регистров Lo байт	0A	Кол-во записанны
02	Количество байт далее	26	Контрольная сумм
CD	Значение байт DO 27-20 (1100 1101)	99	Контрольная сумм
01	Значение байт DO 29-28 (0000 0001)		
BF	Контрольная сумма CRC		
0B	Контрольная сумма CRC		

В ответе возвращается количество записанных регистров.

Как послать команду Modbus RTU на запись нескольких аналоговых выводов? Команда 0x10
Эта команда используется для записи нескольких значений аналогового выхода AO.
Пример записи в несколько AO с регистрами #40002 и #40003 для SlaveID адреса устройства 17. Адрес первого регистра будет 0001 hex = 1, т.к. счет ведется с 0 адреса.

Байт	Запрос	Байт	Отв
(Hex)	Название поля	(Hex)	Название поля
11	Адрес устройства	11	Адрес устройства
10	Функциональный код	10	Функциональный ко
00	Адрес первого регистра Hi байт	00	Адрес первого реги
01	Адрес первого регистра Lo байт	01	Адрес первого реги
00	Количество регистров Hi байт	00	Кол-во записанных
02	Количество регистров Lo байт	02	Кол-во записанных
04	Количество байт далее	12	Контрольная сумма
00	Значение Hi 40002	98	Контрольная сумма
0A	Значение Lo 40002		
01	Значение Hi 40003		
02	Значение Lo 40003		
C6	Контрольная сумма CRC		
F0	Контрольная сумма CRC		

Какие бывают ошибки запроса Modbus?

Если устройство получило запрос, но запрос не может быть обработан, то устройство ответит кодом ошибки.

Ответ будет содержать измененный Функциональный код, старший бит будет равен 1.

Пример:

Было	Стало
Функциональный код в запросе	Функциональный код ошибки
01 (01 hex) 0000 0001	129 (81 hex) 1000 0001
02 (02 hex) 0000 0010	130 (82 hex) 1000 0010
03 (03 hex) 0000 0011	131 (83 hex) 1000 0011
04 (04 hex) 0000 0100	132 (84 hex) 1000 0100
05 (05 hex) 0000 0101	133 (85 hex) 1000 0101
06 (06 hex) 0000 0110	134 (86 hex) 1000 0110
15 (0F hex) 0000 1111	143 (8F hex) 1000 1111
16 (10 hex) 0001 0000	144 (90 hex) 1001 0000

Пример запроса и ответ с ошибкой:

Байт	Запрос	Байт	Ответ

(Hex)	Название поля	(Hex)	Название поля
0A	Адрес устройства	0A	Адрес устройства
01	Функциональный код	81	Функциональный код с изм
04	Адрес первого регистра Hi байт	02	Код ошибки
A1	Адрес первого регистра Lo байт	B0	Контрольная сумма CRC
00	Количество регистров Hi байт	53	Контрольная сумма CRC
01	Количество регистров Lo байт		
AC	Контрольная сумма CRC		
63	Контрольная сумма CRC		

Расшифровка кодов ошибок

01	Принятый код функции не может быть обработан.
02	Адрес данных, указанный в запросе, недоступен.
03	Значение, содержащееся в поле данных запроса, является недопустимой величиной.
04	Невосстанавливаемая ошибка имела место, пока ведомое устройство пыталось выполнить действие.
05	Ведомое устройство приняло запрос и обрабатывает его, но это требует много времени. Э предохраняет ведущее устройство от генерации ошибки тайм-аута.
06	Ведомое устройство занято обработкой команды. Ведущее устройство должно повторить позже, когда ведомое освободится.
07	Ведомое устройство не может выполнить программную функцию, заданную в запросе. Эт возвращается для неуспешного программного запроса, использующего функции с номерами 13 и устройство должно запросить диагностическую информацию или информацию об ошибках от ве
08	Ведомое устройство при чтении расширенной памяти обнаружило ошибку паритета. Веду может повторить запрос, но обычно в таких случаях требуется ремонт.
10 (0A hex)	Шлюз неправильно настроен или перегружен запросами.
11 (0B hex)	Slave устройства нет в сети или от него нет ответа.