

Протокол MODBUS	1
1.1. Протокол MODBUS	1
1.2. Форматы представления параметров в теплосчетчике СТУ-1	1
1.2. Адреса параметров	2
2. Описание протокола	4
2.1. Общие сведения	4
2.2. Режимы передачи	5
2.3. Обнаружение ошибок	6
CRC-16 (Cyclic Redundancy Check)	6
Контрольная сумма LRC	9
Кадровая синхронизация в режиме RTU	9
2.4. Поле адреса	9
2.5. Поле функции	9
2.6. Поле данных	10
2.7. Поле контрольной суммы	10
Исключительные ситуации	12
3. Описание функций протокола	13
3.1. Функция 1: чтение логических ячеек	14
3.2. Функция 2: чтение дискретных входов	15
3.3. Функция 3: чтение регистров	15
3.4. Функция 5: запись одной ячейки	16
3.5. Функция 6: запись одного регистра	16
3.6. Функция 8: тестовая функция	17
3.7. Функция 7: чтение статуса	18
3.8. Функция 16: Запись нескольких регистров	18
3.9. Функция 17: чтение информации об адресуемом устройстве	19
3.10 Пользовательская функция 65, 66, 67, 68: чтение архива	19

Протокол MODBUS

1.1. Протокол MODBUS

Теплосчетчик СТУ-1 для связи через последовательный порт использует протокол связи MODBUS фирмы Gould Modicon, а, в частности, функции 3 и 17.

Для получения накопленных значений объема и наработанного времени используется функция 3.

Для получения информации о приборе используется функция 17.

Режим передачи последовательного канала – 8, N, 1. Скорость обмена по умолчанию – 9600 б/с.

Дополнительные функции архива реализованы начиная с версии 2.

1.2. Форматы представления параметров в теплосчетчике СТУ-1

В приборе СТУ-1 приняты следующие форматы для представления чисел:

Формат int (0x1234)

Адрес	0	1
Содержимое	0x12	0x34

Формат long (0x12345678)

Адрес	0	1	2	3
Содержимое	0x12	0x34	0x56	0x78

Число с плавающей запятой типа float вида

SEEEEEEE EAAAAAAAA BBBBVBVVV CCCCCCCC

, где S – знаковый бит;

E – экспонента со смещением 127;

ABC – нормализованная мантисса. Старший бит всегда равен 1, и, следовательно, не упоминается передается в следующем формате:

Формат float

Адрес	0	1	2	3
Содержимое	BBBB BBBB	CCCC CCCC	EEEE EEEE	EAAA AAAA

1.2. Адреса измеряемых параметров

0000/0001	Мгновенный объемный расход 1 канала G1, м ³ /ч	float
0002/0003	Мгновенный объемный расход 2 канала G2, м ³ /ч	float
0004/0005	Мгновенный объемный расход 3 канала G3, м ³ /ч	float
0006/0007	Мгновенный объемный расход 4 канала G4, м ³ /ч	float
0008/0009	Мгновенный объемный расход 5 канала G5, м ³ /ч	float
000A/000B	Мгновенный объемный расход 6 канала G6, м ³ /ч	float
000C	Температура 1 канала T1, °C	int (T)
000D	Температура 2 канала T2, °C	int (T)
000E	Температура 3 канала T3, °C	int (T)
000F	Температура 4 канала T4, °C	int (T)
0010	Температура 5 канала T5, °C	int(T)
0012	Давление 1 канала P1, МПа	int(P)
0013	Давление 2 канала P2, МПа	int(P)
0014	Давление 3 канала P3, МПа	int(P)
0015	Давление 4 канала P4, МПа	int(P)
0016/0017	Плотность воды 1 канала p1, кг/м ³	float
0018/0019	Плотность воды 2 канала p2, кг/м ³	float
001A/001B	Плотность воды 3 канала p3, кг/м ³	float
001C/001D	Плотность воды 4 канала p4, кг/м ³	float
001E/001F	Мгновенный массовый расход 1 канала Gm1, т/ч	float
0020/0021	Мгновенный массовый расход 2 канала Gm2, т/ч	float
0022/0023	Мгновенный массовый расход 3 канала Gm3, т/ч	float
0024/0025	Мгновенный массовый расход 4 канала Gm4, т/ч	float
0026/0027	Мгновенный массовый расход 5 канала Gm5, т/ч	float
0028/0029	Мгновенный массовый расход 6 канала Gm6, т/ч	float
002A/002B	Мгновенная тепловая мощность 1 тепловвода W1, ГДж/ч	float
002C/002D	Мгновенная тепловая мощность 2 тепловвода W2, ГДж/ч	float
002E/002F/0030/0031	Накопленная тепловая энергия 1 тепловвода E1, ГДж	long/float
0032/0033/0034/0035	Накопленная тепловая энергия 2 тепловвода E2, ГДж	long/float
0036/0037/0038/0039	Накопленный объем 1 канала V1, м ³	long/float
003A/003B/003C/003D	Накопленный объем 2 канала V2, м ³	long/float
003E/003F/0040/0041	Накопленный объем 3 канала V3, м ³	long/float
0042/0043/0044/0045	Накопленный объем 4 канала V4, м ³	long/float
0046/0047/0048/0049	Накопленный объем 5 канала V5, м ³	long/float
004A/004B/004C/004D	Накопленный объем 6 канала V6, м ³	long/float
004E/004F/0050/0051	Накопленная масса 1 канала M1, т	long/float
0052/0053/0054/0055	Накопленная масса 2 канала M2, т	long/float
0056/0057/0058/0059	Накопленная масса 3 канала M3, т	long/float
005A/005B/005C/005D	Накопленная масса 4 канала M4, т	long/float
005E/005F/0060/0061	Накопленная масса 5 канала M5, т	long/float

0062/0063/0064/0065	Накопленная масса 6 канала Мб, т	long/float
006D/006E/006F	Текущее время в приборе, struct SRTClock	Srtclock
0070	Младшее слово регистра нештатных состояний	int
0071	Старшее слово регистра нештатных состояний	int
0066/0067	Время наработки 1 канала, мин	3 байта
0068/0069	Время наработки 2 канала, мин	3 байта
007B/007C/007D/007E	Накопленная энергия 1 канала, Ккал	stotal
007F/0080/0081/0082	Накопленная энергия 2 канала, Ккал	stotal

Значения накопленного объема (накопленной массы, накопленной энергии) представляют две составляющие типа long и float. В четырех первых байтах содержится целая часть значения (long), в остальных четырех – вещественная (float).

Накопленное время наработки хранится в младших 3 байтах, в минутах.

Текущее время передается в следующем формате:

006D	Год (00-99) / месяц (1-12)
006E	День(1-31)/--
006F	Час(0-23)/Минута (0-59)

Температура передается в целочисленном формате размером в 2 байта приведенное к 151. Температуре 0⁰С соответствует значение 0, 151⁰С соответствует значение 0xFFFF.

Аналогично температуре передается значение давления, причем это значение приведено к 1,6.

Описание регистра нештатных состояний:

1 бит (младший) - "P1B" –измеренный расхода 1 канала превышает договорный расход 1 канала

2 бит - "P1H" – измеренный расход 1 канала ниже минимального расхода 1 канала

3 бит - "P2B" - измеренный расхода 2 канала превышает договорный расход 2 канала

4 бит - "P2H" - измеренный расход 2 канала ниже минимального расхода 2 канала

5 бит - "M12" – дисбаланс измеренных масс 1 и 2 каналов (только в закрытых системах)

6 бит - "P1" – отказ по расходу 1 канала

7 бит - "P2" – отказ по расходу 2 канала

8 бит - "P5" – отказ по расходу 5 канала

9 бит - "P3B"- измеренный расхода 3 канала превышает договорный расход 3 канала

10 бит - "P3H"- измеренный расход 3 канала ниже минимального расхода 3 канала

11 бит - "P4B"- измеренный расхода 4 канала превышает договорный расход 4 канала

12 бит - "P4H" - измеренный расход 4 канала ниже минимального расхода 4 канала

13 бит -"M34" – дисбаланс измеренных масс 3 и 4 каналов (только для закрытых систем)

14 бит - "P3" – отказ по расходу 3 канала

15 бит - "P4" – отказ по расходу 4 канала

16 бит - "P6" – отказ по расходу 6 канала

17 бит - "P5B" - измеренный расхода 5 канала превышает договорный расход 5 канала

18 бит - "P5H" - измеренный расход 5 канала ниже минимального расхода 5 канала

19 бит - "P6B" - измеренный расхода 6 канала превышает договорный расход 6 канала,

20 бит - "P6H" - измеренный расход 6 канала ниже минимального расхода 6 канала

21 бит - "T1" – отказ температуры 1 канала

22 бит - "T2" – отказ температуры 2 канала

23 бит - "T3" – отказ температуры 3 канала

24 бит - "T4" – отказ температуры 4 канала

25 бит - "T1H" – измеренная температура 1 канала ниже договорной темп. 1 канала

26 бит - "T2B" – измеренная температура 2 канала превышает договорную темп 2 канала

27 бит - "T3H" – измеренная температура 3 канала ниже договорной темп. 3 канала

28 бит - "Т4В" – измеренная температура 4 канала превышает договорную темп 4 канала
32 бит (старший) – “БП” – теплосчетчик находился без питания.

1.3. Адреса настроечных параметров

8048/8049	Максимальный расход 1 канала $G1dog$, м ³ /ч	float
804A/804B	Внутренний диаметр 1 канала $D1$, м	float
804C/804D	База датчиков 1 канала $L1$, м	float
804E/804F	Смещение нуля $Z1$, нс	float
8050/8051	Длина кабеля $Lk1$, м	float
8052/8053	Гидродинамический коэффициент $K1$	float
8054/8055	Минимальный расход 1 канала $G1min$, м ³ /ч	float
8056/8057	Отсечка 1 канала $Go1$, м ³ /ч	float
8069/806A	Цена импульса 3 канала, м ³ /имп	float
806B/806C	Максимальный расход 3 канала, м ³ /ч	float
806D/806E	Минимальный расход 3 канала, м ³ /ч	float
8076/8077	Цена импульса 5 канала, м ³ /имп	float
8078/8079	Максимальный расход 5 канала, м ³ /ч	float
807A/807B	Минимальный расход 5 канала, м ³ /ч	float
0x80AB	Схема	младший байт
0x8046	Температура холодной воды Tx = ст. байт/100 оС, давление холодной воды Px = мл. байт/100 МПа	int

2. Описание протокола

Данный документ является сокращенным переводом описания стандартного протокола MODBUS фирмы MODICON. Исходный текст на английском языке можно получить по URL: <http://www.modicon.com/techpubs/toc7.html>.

2.1. Общие сведения

Протокол необходимая часть работы системы. Он определяет как Мастер (MS) и Slave (SL) устанавливают и прерывают контакт, как идентифицируются отправитель и получатель, каким образом происходит обмен сообщениями, как обнаруживаются ошибки. Протокол управляет циклом запроса и ответа, который происходит между устройствами MS и SL, как показано на рисунке.

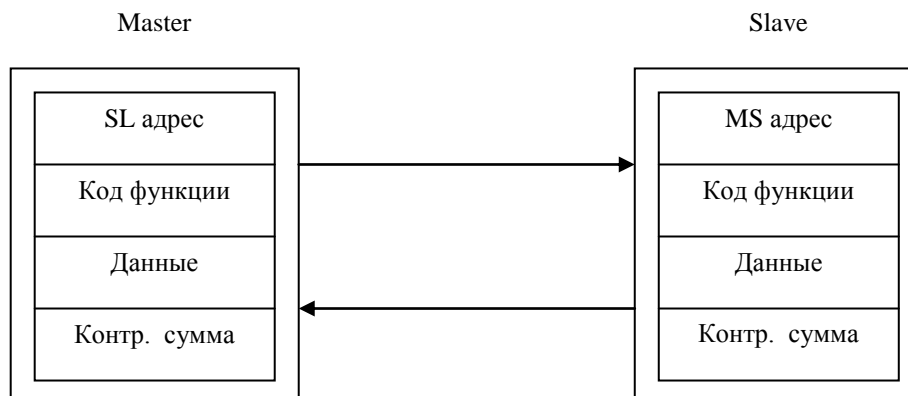


Рис.1.

Протокол подразумевает на общей шине один MS и до 247 SL. Хотя протокол и поддерживает до 247 SL, некоторые приборы ограничивают число SL, подключаемых к общей шине. Например, драйвер шины теплосчетчика СТУ-1 и позволяет подключить к одному сегменту двухпроводной линии RS485 максимум 32 прибора. Каждому SL присвоен уникальный адрес устройства в диапазоне от 1 до 32.

Только MS может инициировать транзакцию. Транзакции бывают либо типа запрос/ответ (адресуется только один SL), либо широковещательные/без ответа (адресуются все SL). Транзакция содержит один кадр запроса и один кадр ответа, либо один кадр широковещательного запроса. В теплосчетчике СТУ-1 использовать широковещательный запрос проводить не рекомендуется.

Некоторые характеристики протокола MODBUS фиксированы. К ним относятся формат кадра, последовательность кадров, обработка ошибок коммуникации и исключительных ситуаций, и выполнение функций.

Другие характеристики выбираются пользователем. К ним относятся тип средства связи, скорость обмена, проверка на четность и число стоповых бит. Параметры, выбираемые пользователем, устанавливаются (аппаратно или программно) на каждой станции. Эти параметры не могут быть изменены во время работы системы.

При передаче по линиям данных, сообщения помещаются в «конверт». «Конверт» покидает устройство через «порт» и «пересылается» по линиям адресуемому устройству. Протокол Modbus описывает «конверт» в форме кадров сообщений. Информация в сообщении представляет адрес требуемого получателя, что получатель должен сделать, данные, необходимые для выполнения этого, и механизм контроля достоверности.

Когда сообщение достигает интерфейса SL, оно попадает в адресуемое устройство через похожий «порт». Адресуемое устройство вскрывает конверт, читает сообщение, и, если не возникло ошибок, выполняет требуемую задачу. Затем оно помещает в конверт ответное сообщение и посылает его отправителю. Информация в ответном сообщении представляет собой адрес адресуемого устройства, выполненную задачу, данные, полученные в результате выполнения задачи, и механизм контроля достоверности. Если сообщение было широковещательным (сообщение для всех SL) на что указывает адрес 0, то ответное сообщение не передается.

В большинстве случаев, MS посылает следующее сообщение другому SL либо после приема корректного ответного сообщения, либо после прохождения определенного пользователем интервала времени, если ответное сообщение не было получено. Все сообщения могут рассматриваться как запросы, генерирующие ответные сообщения от SL. Широковещательные сообщения могут рассматриваться как запросы, не требующие ответных сообщений от SL.

2.2. Режимы передачи

Режим передачи определяет структуру отдельных блоков информации в сообщении и системы счисления, используемую для передачи данных. В системе Modbus существуют два режима передачи. Оба режима обеспечивают одинаковую совместимость при связи с SL. Режим выбирается в зависимости от оборудования, используемого как Master Modbus. Для каждой системы Modbus должен использоваться только один режим. Смешивание режимов не разрешительно. Режимы делятся на ASCII и RTU (Remote Terminal Unit).

Таблица 1.

Характеристики режимов ASCII и RTU

Характеристика	ASCII (7-бит)	RTU (8-бит)
Система кодирования	Используются ASCII символы 0-9, A-F	8-битовая двоичная система
Число бит на символ		
Стартовые биты	1	1
Биты данных (LSB вперед)	7	8
Четность	Вкл./Выкл.	Вкл./Выкл.
Стоповые биты	1 или 2	1 или 2

Контрольная сумма	LRC (Longitudinal Redundancy Check)	CRC (Cyclical Redundancy Check)
-------------------	-------------------------------------	---------------------------------

Символы ASCII удобнее использовать при отладке, поэтому этот режим удобен для компьютеров, программируемых на языке высокого уровня. Режим RTU подходит для компьютеров, программируемых на машинных языках.

В режиме RTU данные передаются в виде 8-ми разрядных двоичных символов. В режиме ASCII каждый RTU символ сначала делится на две 4-х разрядных части (старший и младший), переводится в свой шестнадцатеричный эквивалент и затем используется в создании сообщения. ASCII режим использует в два раза больше символов, чем RTU режим, но декодирование и управление данными легче. К тому же, в режиме RTU символы сообщения должны передаваться непрерывным потоком. В режиме ASCII допустима задержка до 1 секунды между двумя соседними символами.

Во всех приборах фирмы ЗАО «ТЕСС-Инжиниринг», поддерживающих протокол Modbus, реализованы оба режима.

2.3. Обнаружение ошибок

Существует два типа ошибок, которые могут возникать в системах связи: ошибки передачи и программные или оперативные ошибки. Система Modbus имеет способы определения каждого типа ошибок.

Ошибки связи обычно заключаются в изменении бита или бит сообщения. Например, байт 0001 0100 может измениться на 0001 0110. Ошибки связи выявляются при помощи символа кадра, контроля по четности и избыточным кодированием.

Когда обнаруживается ошибка кодирования, четности и контрольной суммы, обработка сообщения прекращается. SL не должен генерировать ответное сообщение. (Тот же результат достигается, если был использован адрес несуществующего SL).

Если возникает ошибка связи, данные сообщения ненадежны. Устройство SL не может с уверенностью определить, что сообщение было адресовано именно ему. Иначе SL может ответить сообщением, которое не является ответом на исходный запрос. Устройство MS должно программироваться так, чтобы в случае не получения ответного сообщения в течении определенного времени, MS должен фиксировать ошибку связи. Продолжительность этого времени зависит от скорости обмена, типа сообщения, и времени опроса SL. По истечению этого периода, MS должен быть запрограммирован на ретрансляцию сообщения.

Оба режима передачи, RTU и ASCII, могут включать в формат символа дополнительный бит четности. В режиме RTU это девятый бит данных в поле данных (8 бит данных и бит четности). В режиме ASCII это восьмой бит данных (7 бит данных и бит четности). Если контроль четности не используется, бит четности не передается. Все устройства в системе должны быть сконфигурированы одинаково.

Контроль четности может определить только изменение одного бита символа. Изменение двух битов в символе контроль четности определить не в состоянии.

Для обеспечения качества передачи данных система Modbus обеспечивает несколько уровней обнаружения ошибок. Для обнаружения множественного изменения битов сообщения система использует избыточный контроль: CRC и LRC. Какой контроль использовать зависит от режима передачи. RTU использует CRC, а ASCII использует LRC. Расчет CRC описан ниже. Обнаружение ошибок с помощью CRC и LRC выполняется автоматически.

CRC-16 (Cyclic Redundancy Check)

Сообщение (только биты данных, без учета старт/стоповых бит и бит четности) рассматривается как одно последовательное двоичное число, у которого старший значащий бит (MSB) передается первым. Сообщение умножается на X^{16} (сдвигается влево на 16 бит), а затем делится на $X^{16}+X^{15}+X^2+1$, выражаемое как двоичное число (11000000000000101). Целая часть результата игнорируется, а 16-битный остаток (предварительно инициализированный единицами для предотвращения случая, когда все сообщение состоит из нулей) добавляется к сообщению (старшим битом вперед) как два байта контрольной суммы. Полученное сообщение, включающее CRC, затем в приемнике делится на тот же полином ($X^{16}+X^{15}+X^2+1$). Если ошибок не было, остаток от деления должен получиться нулевым. (Приемное устройство может рассчитать CRC и сравнить ее с переданной). Вся арифметика выполняется по модулю 2 (без переноса).

Устройство, используемое для подготовки данных для передачи, посылает условно самый правый бит (LSB) каждого символа первым. При расчете CRC, первый передаваемый бит, определен как MSB делимого. Так как арифметика не использует перенос, для удобства расчета CRC, можно предположить, что MSB расположен справа. Поэтому порядок бит при расчете полинома должен быть реверсивным. MSB полинома опускается, так как он влияет только на делитель, а не на остаток. В результате получается 1010 0000 0000 0000 0001 (A001H). Заметьте, что эта реверсивность порядка бит, в любом случае не влияет на интерпретацию или порядок бит в байте данных при вычислении CRC.

Пошаговая процедура расчета CRC-16 представлена ниже:

1. Загрузить 16-ти разрядный регистр числом FFFFH.
2. Выполнить операцию XOR над первым байтом данных и старшим байтом регистра.

Поместить результат в регистр.

3. Сдвинуть регистр на один разряд вправо.
4. Если выдвинутый вправо бит единица, выполнить операцию XOR между регистром и полиномом 1010 0000 0000 0001 (A001H).
5. Если выдвинутый бит ноль, вернуться в шаг 3.
6. Повторять шаги 3 и 4 до тех пор, пока не будут выполнены 8 сдвигов регистра.
7. Выполнить операцию XOR над следующим байтом данных и регистром.
8. Повторять шаги 3-7 до тех пор, пока не будут выполнены операция XOR над всеми байтами данных и регистром.
9. Содержимое регистра представляет собой два байта CRC и добавляется к исходному сообщению старшим битом вперед.

Таблица 2

Пример расчета CRC для сообщения - чтение статуса SL с номером 02

16-ти разрядный регистр				MSB	Флаг
Исключающее ИЛИ	1111	1111	1111	1111	
02			0000	0010	
	1111	1111	1111	1101	
Сдвиг 1	0111	1111	1111	1110	1
Полином	1010	0000	0000	0001	
	1101	1111	1111	1111	
Сдвиг 2	0110	1111	1111	1111	1
Полином	1010	0000	0000	0001	
	1100	1111	1111	1110	
Сдвиг 3	0110	0111	1111	1111	
Сдвиг 4	0011	0011	1111	1111	1
Полином	1010	0000	0000	0001	
	1001	0011	1111	1110	
Сдвиг 5	0100	1001	1111	1111	
Сдвиг 6	0010	0100	1111	1111	1
Полином	1010	0000	0000	0001	
	1000	0100	1111	1110	
Сдвиг 7	0100	0010	0111	1111	
Сдвиг 8	0010	0001	0011	1111	1
Полином	1010	0000	0000	0001	
	1000	0001	0011	1110	
07			0000	0111	
	1000	0001	0011	1001	
Сдвиг 1	0100	0000	1001	1100	1
Полином	1010	0000	0000	0001	
	1110	0000	1001	1101	
Сдвиг 2	0111	0000	0100	1110	1
Полином	1010	0000	0000	0001	
	1101	0000	0100	1111	
Сдвиг 3	0110	1000	0010	0111	1
Полином	1010	0000	0000	0001	
	1100	1000	0010	0110	
Сдвиг 4	0110	0100	0001	0011	
Сдвиг 5	0011	0010	0000	1001	1
Полином	1010	0000	0000	0001	
	1001	0010	0000	1000	
Сдвиг 6	0100	1001	0000	0100	
Сдвиг 7	0010	0100	1000	0010	
Сдвиг 8	0001	0010	0100	0001	

Таблица 3

16-ти разрядный регистр		MSB		Флаг
HEX 12		1 HEX 41		
Передаваемое сообщение с контрольной суммой CRC- 16 (При передаче сообщение выдвигается вправо)				
12	41	07	02	
0001 0010	0100 0001	0000 0111	0000 0010	
Последний бит	Порядок передачи		Первый бит	

Контрольная сумма LRC.

Метод LRC проверяет содержание сообщения исключая начальный символ ":" и пару CRLF.

LRC это 1 байт. LRC вычисляется передающим устройством и добавляется в конец сообщения. Принимающее устройство вычисляет LRC в процессе приема сообщения и сравнивает его с принятым от главного. Если есть несовпадение, то имеет место ошибка.

Кадровая синхронизация в режиме RTU

В режиме RTU кадровая синхронизация может поддерживаться только путем эмулирования синхронного сообщения. Приемное устройство отслеживает время между приемом символов. Если прошло время, равное периоду следования 3.5 символов, а кадр не был завершен или не поступило нового символа, устройство очищает кадр и предполагает, что следующий принимаемый байт - это адрес устройства в новом сообщении.

Таблица 5

Формат кадра сообщения в режиме RTU

T1 T2 T3	Адрес	Функция	Данные	Контрольная сумма	T1 T2 T3
	8 бит	8 бит	N * 8 бит	16 бит	

2.4. Поле адреса

Поле адреса следует сразу за началом кадра и состоит из одного 8-ми разрядного символа в режиме RTU. Эти биты указывают пользователю адрес SL устройства, которое должно принять сообщение, посланное MS.

Каждый SL должен иметь уникальный адрес и только адресуемое устройство может ответить на запрос, который содержит его адрес. Когда SL посылает ответ, адрес SL информирует MS, с какой SL на связи. В широкоэвещательном режиме используется адрес 0. Все SL интерпретируют такое сообщение как выполнение определенного действия, но без посылки подтверждения.

2.5. Поле функции

Поле кода функции указывает адресуемому SL какое действие выполнить. Коды функций Modbus специально разработаны для связи ПК и промышленных коммуникационных систем Modbus.

Старший бит этого поля устанавливается в единицу SL в случае, если он хочет просигнализировать MS, что ответное сообщение не нормальное. Этот бит остается в нуле, если ответное сообщение повторяет запрос или в случае нормального сообщения.

Таблица 6

Коды функций Modbus		
Код	Название	Действие
01	READ COIL STATUS	Получение текущего состояния (ON/OFF) группы логических ячеек.

Код	Название	Действие
02	READ INPUT STATUS	Получение текущего состояния (ON/OFF) группы дискретных входов.
03	READ HOLDING REGISTERS	Получение текущего значения одного или нескольких регистров хранения.
04	READ INPUT REGISTERS	Получение текущего значения одного или нескольких входных регистров.
05	FORCE SINGLE COIL	Изменение логической ячейки в состояние ON или OFF.
06	FORCE SINGLE REGISTER	Запись нового значения в регистр хранения.
07	READ EXCEPTION STATUS	Получение состояния (ON/OFF) восьми внутренних логических ячеек, чье назначение зависит от типа контроллера. Пользователь может использовать эти ячейки по своему выбору.
08	LOOPBACK DIAGNOSTIC TEST	Тестовое сообщение, посылаемое SL для получения данных о связи.
11	FETCH EVENT COUNTER COMMUNICATIONS	Позволяет MS путем последовательной отправки одного сообщения определить выполнение операции.
12	FETCH COMMUNICATIONS EVENT LOG	Позволяет MS получить журнал связи, который содержит информацию о каждой Modbus транзакции данного SL. Если транзакция не выполнена, в журнал заносится информация об ошибке.
13	PROGRAM	Позволяет MS запрограммировать SL.
14	POLL PROGRAM COMPLETE	Позволяет MS связываться с другими SL если один SL выполняет долговременную операцию программирования SL периодически опрашивается на момент завершения программирования Данный запрос посылается только в том случае, если предварительно был послан запрос PROGRAM.
15	FORCE MULTIPLE COILS	Изменить состояние (ON/OFF) нескольких последовательных логических ячеек.
16	FORCE MULTIPLE REGISTERS	Установить новые значения нескольких последовательных регистров.
17	REPORT SLAVE I.D.	Позволяет MS определить тип адресуемого SL и его рабочее состояние.
19	RESET COMMUNICATIONS LINK	Сбрасывает SL в известное состояние после неустранимой ошибки. Сбрасывает счетчик принятых байт.
20-64	Зарезервировано под расширения Modbus	
65-72	Зарезервировано под пользовательские функции.	В дальнейшем не будет использоваться в продуктах Modicon.
73-119	ILLEGAL FUNCTION	
120-127	Зарезервировано	Зарезервировано Modicon для внутреннего использования.
128-255	Зарезервировано	Зарезервировано для исключительных ситуаций.

2.6. Поле данных

Поле данных содержит информацию, необходимую SL для выполнения указанной функции, или содержит данные собранные SL для ответа на запрос.

2.7. Поле контрольной суммы

Это поле позволяет MS и SL проверять сообщение на наличие ошибок. Иногда, вследствие электрических помех или других воздействий, сообщение при пересылке от одного устройства к другому может незначительно измениться. Результат проверки контрольной суммы укажет SL или MS реагировать или не реагировать на такое сообщение. Это увеличивает надежность и эффективность систем MODBUS.

В режиме ASCII в поле контрольной суммы используется LRC, а в режиме RTU - CRC.

Если сообщения запроса и ответа могли бы читаться по-английски, то четыре поля этих сообщений выглядели как на рисунке 1. (Заметьте, что последовательность посылки полей каждый раз одна и та же - Адрес, Код функции, Данные и Контрольная сумма - независимо от направления).

Таблица 7

MODBUS MS	ERROR CHECK	DATA	FUNCTION CODE (03)	ADDRESS (01)	MODBUS SL
→	Информация используется приемным устройством для проверки сообщения	Относительный адрес регистра	Чтение регистра хранения	Запрос для SL с номером 1	→
	ADDRESS (01)	FUNCTION CODE (03)	DATA	ERROR CHECK	
←	Ответ от SL с номером 1	Чтение регистра хранения	Значение, содержащееся в указанном регистре хранения	Информация, используемая приемным устройством для проверки сообщения	←

Исключительные ситуации

Коды исключительных ситуаций приведены в таблице 8. Когда SL обнаруживает одну из этих ошибок, он посылает ответное сообщение MS, содержащее адрес SL, код функции, код ошибки и контрольную сумму. Для указания на то, что ответное сообщение - это уведомление об ошибке, старший бит поля кода функции устанавливается в 1. Таблице 9 и 10 представлен пример некорректного запроса и соответствующего ответа с кодом исключительной ситуации.

Таблица 8

Код	Название	Смысл
01	ILLEGAL FUNCTION	Функция в принятом сообщении не поддерживается на данном SL. Если тип запроса - POLL PROGRAM COMPLETE, этот код указывает, что предварительный запрос не был командой программирования
02	ILLEGAL DATA ADDRESS	Адрес, указанный в поле данных, является недопустимым для данного SL.
03	ILLEGAL DATA VALUE	Значения в поле данных недопустимы для данного SL.
04	FAILURE IN ASSOCIATED DEVICE	SL не может ответить на запрос или произошла авария.
05	ACKNOWLEDGE	SL принял запрос и начал выполнять долговременную операцию программирования. Для определения момента завершения операции используйте запрос типа POLL PROGRAM COMPLETE. Если этот запрос был послан до завершения операции программирования, то SL ответит сообщением REJECTED MESSAGE.
06	BUSY, REJECTED MESSAGE	Сообщение было принято без ошибок, но SL в данный момент выполняет долговременную операцию программирования. Запрос необходимо ретранслировать позднее.
07	NAK-NEGATIVE ACKNOWLEDGMENT	Функция программирования не может быть выполнена. Используйте опрос для получения детальной аппаратно-зависимой информации об ошибке.

Таблица 9

Адрес SL	Функция	Старший байт адреса	Младший байт адреса	Старший байт числа ячеек	Младший байт числа ячеек	Контрольная сумма
0A	01	04	A1	00	01	4F

Этот запрос требует состояние ячейки с номером 1245 в SL с номером 10, и если этот контроллер имеет 1К ячеек, то этот адрес является ошибочным. Соответственно, будет сгенерировано следующее ответное сообщение.

Таблица 10

Адрес SL	Функция	Код исключительной ситуации	Контрольная сумма	
0A	81	02	21	E0

Значение в поле функции равно оригинальному значению с установленным в единицу старшим битом. Код исключительной ситуации 02 указывает на ошибочный адрес данных.

3. Описание функций протокола

Цель данного раздела - определить общий формат соответствующих команд, доступных программисту системы MODBUS. В разделе описаны формат каждого запросного сообщения, выполняемая функция и формат нормального ответного сообщения.

Сообщения с номерами функций 1-6, 15 и 16 ссылаются на конкретные доступные переменные программируемого контроллера. Функция 1, 5 и 15 ссылаются на логические ячейки (OXXX(X)), функция 2 на дискретные входы (1XXX(X)), функция 4 на входные регистры (ZXXX(X)), функции 3,6 и 16 на внутренние регистры (4XXX(X)). Все адреса ссылок в сообщениях MODBUS индексируются с нуля.

Примеры в данном разделе демонстрируют протокол независимо от режима RTU или ASCII. Для корректировки пакета, в зависимости от режима передачи, программист может использовать метод, описанный ниже.

Во всем разделе протокол будет представлен по возможности в формате, указанном на Рис. 1. Числа имеют шестнадцатеричный формат.

Таблица 11

Адрес	Функция	Старший байт адреса первого регистра	Младший байт адреса первого регистра	Старший байт числа требуемых регистров	Младший байт числа требуемых регистра	Поле контрольной суммы	
06	03	00	6B	00	03	89	CRC16

Данный пример описывает чтение регистров 4108-4110 из SL с адресом 06. Это сообщение при форматировании в RTU и ASCII выглядит следующим образом:

Таблица 12

ЗАПРОС	RTU		ASCII	
Заголовок				:
Адрес	0000	0110	0	6
Функция	0000	0011	0	3
Начальный адрес	H.O.	0000	0000	0
	L.O.	0110	1011	6
Количество требуемых регистров	H.O.	0000	0000	0
	L.O.	0000	0011	0
Поле контрольной суммы		1101	1101	8
		0101	0001	
Trailer			CR	LF

ЗАПРОС		RTU		ASCII	
ОТВЕТ		RTU		ASCII	
Заголовок					
Адрес		0000	0110	0	6
Функция		0000	0011	0	3
Количество байт данных		0000	0110	0	6
Данные	H.O.	0000	0010	0	2
	L.O.	0010	1011	2	B
	H.O.	0000	0000	0	0
	L.O.	0000	0000	0	0
	H.O.	0000	0000	0	0
	L.O.	0110	0011	6	3
Контрольная сумма		CRC		6	1
Trailer				CR	LF
Длина пакета		11 байт		23 байта	

3.1. Функция 1: чтение логических ячеек

Запрос.

Функция позволяет пользователю получить статус (1 /0) логических ячеек. Широковещательный режим не поддерживается. Помимо полей адреса SL и функции, сообщение требует, чтобы информационное поле содержало логический адрес первой ячейки и число ячеек, статус которых необходимо получить.

Адресация позволяет получить за один запрос до 2000 логических ячеек. Однако, некоторые приборы имеют ограничение на максимальное число ячеек, статус которых можно получить за один запрос. Ячейки нумеруются с нуля (ячейка 1 = 0, ячейка 2 = 1 и т.д.).

Ниже представлен запрос на чтение логических ячеек 0020 - 0056 из прибора с адресом 17.

Таблица 13

Адрес	Функция	Старший байт адреса первой ячейки	Младший байт адреса первой ячейки	Старший байт число ячеек	Младший байт числа ячеек	Контрольная сумма	
11	01	00	13	00	25	B6	CRC16

Ответ.

Ниже представлен пример ответного сообщения на предыдущий запрос.

Таблица 14

Адрес	Функция	Количество байт в поле данных	Статус ячеек 20-27	Статус ячеек 28-35	Статус ячеек 36-43	Статус ячеек 44-51	Статус ячеек 52-56	Контрольная сумма	
11	01	05	CD	6B	B2	0E	1B	2D	DE

Данные в поле данных упакованы - один бит на каждую ячейку. Ответное сообщение включает адрес SL, код функции, число байт в поле данных, данные и контрольную сумму. Младший значащий бит первого байта поля данных содержит первую адресуемую ячейку, за которой следуют остальные. Если число ячеек не кратно 8-ми, то остальные биты заполняются нулями в порядке от старших битов к младшим.

Статус ячеек 20 - 27 равен CDH = 1101 1101. Читая слева направо, видим, что ячейки 27, 26, 23, 22 и 20 установлены. Остальные данные разбираются так же. Так как было запрошено число ячеек не кратное 8-ми, старшие три бита в последнем байте данных (1BH) заполнены нулями.

Так как запрос обслуживается в конце рабочего цикла прибора, то данные в ответном сообщении отражают состояние ячеек на тот момент.

3.2. Функция 2: чтение дискретных входов

Запрос.

Данная функция позволяет пользователю получить состояние (ВКЛ/ВЫКЛ) входных дискретных линий адресуемого SL. Широковещательный запрос не поддерживается. В дополнение к адресу SL и номеру функции, запрос требует, чтобы информационное поле содержало начальный адрес и количество требуемых линий.

Адресация позволяет получить за один запрос до 2000 линий. Однако, некоторые устройства имеют ограничение на максимальное количество линий, получаемых за один запрос. Входные линии нумеруются с нуля (10001 = 0; 10002 = 1 и т.д.).

В таблице 15 представлен пример запроса на чтение дискретных входов 10197-10218 из SL с номером 17.

Таблица 15

Адрес	Функция	Старший байт номера первой требуемой ячейки	Младший байт номера первой требуемой ячейки	Старший байт количество требуемых ячеек	Младший байт количество требуемых ячеек	Контрольная сумма	
11	02	00	C4	00	16	CRC16	CRC16

Ответ.

Ответное сообщение включает адрес SL, код функции, количество байт данных, данные и поле контрольной суммы. Данные упакованы по биту на каждый вход (1 = ON, 0 = OFF). Младший бит первого байта содержит значение первого адресуемого входа, за которым следуют остальные. Если количество запрошенных входов не кратно 8, то остальные биты заполняются нулями. Количество байт данных всегда определяется как количество RTU данных.

Так как SL обслуживает запрос в конце рабочего цикла, данные в ответе отражают состояние входов на данный момент. Некоторые устройства имеют ограничение на максимальное количество входов, запрашиваемых за один запрос.

Таблица 16

Адрес	Функция	Количество байт данных	Дискретные входы 10197-10204	Дискретные входы 10205-10212	Дискретные входы 10213-10218	Контрольная сумма	
11	02	03	AC	DB	35	CRC16	CRC16

Статус входов 10197-10204 = ACh = 1010 1100. Читая слева направо, видим, что входы 10204, 10202, 10200 и 10199 в состоянии ON. Все остальные байты данных распаковываются аналогично.

Так как было запрошено 22 линии, последний байт данных (35h = 0011 0101) содержит только 6 входов (10213-10218) вместо 8-ми. Два последних бита заполняются нулями.

3.3. Функция 3: чтение регистров

Запрос.

Данная функция позволяет получить двоичное содержимое 16-ти разрядных регистров адресуемого SL. Адресация позволяет получить за каждый запрос до 125 регистров. Однако, некоторые устройства имеют ограничение на максимальное количество регистров, получаемых за один запрос. Регистры нумеруются с нуля.

Широковещательный режим не допускается.

Ниже представлен пример запроса на чтение регистров 108-110 из SL с адресом 17.

Таблица 17

Адрес	Функция	Номер первого регистра		Число регистров для чтения (N)		
		Старший байт	Младший байт	Старший байт	Младший байт	
11	03	00	6B	00	03	CRC16

Ответ.

Адресуемый SL посылает в ответе свой адрес, код выполненной функции и информационное поле. Информационное поле содержит 2 байта, описывающих количество возвращаемых байт данных. Длина каждого регистра данных - 2 байта. Первый байт данных в посылке является старшим байтом регистра, второй - младшим.

Так как SL обычно обслуживает запрос в конце своего рабочего цикла, данные в ответе отражают содержимое регистров в данный момент. Некоторые SL ограничивают количество регистров, передаваемых за один запрос. В этом случае для получения большего числа регистров, необходимо выполнить несколько последовательных запросов.

Ниже представлен пример ответного сообщения на чтение регистров 108-110, имеющих содержимое, соответственно, 555, 0, 100, из SL с адресом 17.

Таблица 18

Адрес	Функция	Количество байт данных	Старший байт регистра 108	Младший байт регистра 108	Старший байт регистра 109	Младший байт регистра 109	Старший байт регистра 110	Младший байт регистра 110	
11	03	06	02	2B	00	00	00	64	CRC16

3.4. Функция 5: запись одной ячейки

Запрос.

Это сообщение модифицирует одну логическую ячейку. Ячейки нумеруются с нуля (ячейка 1 = 0, ячейка 2 = 1 и т.д.). Число 65280 (FF00H) устанавливает ячейку в 1, а число 0 - в 0. Другие числа не влияют на содержимое ячейки. Данная функция может использоваться в широковещательном режиме.

Ниже приведен пример установки в 1 ячейки 0173 в SL 17.

Таблица 19

Адрес	Функция	Старший байт адреса ячейки	Младший байт адреса ячейки	Индикатор установки или сброс ячейки	Всегда 0	Контрольная сумма	
И	05	00	AC	FF	00	CRC16	CRC16

Ответ.

Нормальное ответное сообщение полностью совпадает с запросом.

3.5. Функция 6: запись одного регистра

Запрос.

Данная функция позволяет модифицировать содержимое одного регистра. Хотя запрос и является асинхронным, SL изменяет содержимое регистра только в конце рабочего цикла.

Когда в запросе указан адрес равный 0 (широковещательный запрос), все SL, подключенные к шине, загрузят соответствующий регистр указанным значением.

ПРИМЕЧАНИЕ: В широковещательном режиме используются только функции 5, 6, 15 и 16.

Ниже приведен пример записи регистра 136 значением 926 в SL с номером 17.

Таблица 20

Адрес	Функция	Старший байт адреса регистра 136	Младший байт адреса регистра 136	Старший байт значения 926	Младший байт значения 926	Контрольная сумма	
11	06	00	87	03	9E	CRC16	CRC16

Ответ.

В случае успешного выполнения функции ответное сообщение идентично запросу.

3.6. Функция 8: тестовая функция

Запрос.

Данная функция предназначена для проверки коммуникационной системы и не влияет на данные прибора.

Поле информации содержит 2 байта диагностического кода, указывающего SL выполнить определенное действие и 2 байта необходимой, для данной диагностики, информации.

Таблица 21

Код	Действие
00	Вернуть запрос
01	Сбросить установки связи (без ответа)
02	Вернуть регистр диагностики
03	Изменить символ начала пакета
04	Перевести SL в режим прослушивания линии без посылки ответных сообщений (Listen Only Mode)
05	Сбросить счетчики и регистр диагностики
06	Вернуть счетчик сообщений, полученных с шины MODBUS
07	Вернуть счетчик сообщений с неправильными контрольными суммами
08	Вернуть счетчик сообщений, вызвавших исключительную ситуацию
09	Вернуть счетчик сообщений, адресованных только данному SL
10	Вернуть счетчик сообщений, адресованных данному SL и оставленных без ответа
11	Вернуть счетчик сообщений, адресованных данному SL и вызвавшим исключительную ситуацию NACK
12	Вернуть счетчик сообщений, адресованных данному SL и вызвавшим исключительную ситуацию BUSY

Ниже дан пример запроса вернуть эхо (диагностический код 0) SL с номером 17.

Таблица 22

Адрес	Функция	Старший байт диагностического кода	Младший байт диагностического кода	Старший байт данных ⁹	Младший байт данных	Контрольная сумма	
11	08	00	00	00	00	0B	LRC

⁹В поле данных помещается необходимая для данного запроса информация.

Ответ.

Таблица 23

Адрес	Функция	Старший байт диагностического кода	Младший байт диагностического кода	Старший байт данных ¹⁰	Младший байт данных	Контрольная сумма	
11	08	00	00	00	00	0B	LRC

3.7. Функция 7: чтение статуса

Запрос.

Во многих случаях, для быстрого получения статуса некоторых событий контроллера, желательно иметь в протоколе сообщение, имеющее небольшой размер. Данная функция разработана именно для этой цели.

Функция с номером 7 позволяет пользователю опрашивать состояние восьми ячеек контроллера. Эти ячейки могут программироваться для хранения информации состояния контроллера. Широковещательный режим не поддерживается.

Назначение этих ячеек зависит от типа контроллера.

Ниже представлен пример запроса статуса SL с номером 17.

Таблица 24

Адрес	Функция	Контрольная сумма	
11	07	E8	LRC

В этой функции не требуется поле данных.

Ответ.

Нормальный ответ содержит статус восьми ячеек, упакованных в один байт данных.

Таблица 25

Адрес	Функция	Данные ячеек	Контрольная сумма	
11	07	6D	7B	LRC

В приборах ЗАО "ТЕСС - Инжиниринг" постоянно используются два младших разряда регистра статуса, которые отражают состояние прибора во время программирования памяти программ прибора.

3.8. Функция 16: Запись нескольких регистров

Запрос.

Данное сообщение меняет содержимое любого регистра опрашиваемого контроллера. Сообщение позволяет записывать регистры с максимальным логическим адресом до FFFFH. Неиспользуемые старшие биты адреса регистра должны заполняться нулями. Если используется адрес SL равный 0, то содержимое поля данных записывается во все устройства, подключенные к шине (широковещательный режим).

Ниже дан пример записи в SL с номером 17 двух регистров 136, 137 значениями 0x000A, 0x0102.

¹⁰В поле данных помещается необходимая для данного ответа информация.

Таблица 26

Адрес	Функция	Старший байт адреса первого регистра	Младший байт адреса первого регистра	Количество регистров	Количество байт в поле данных	Старший байт регистра 136	Младший байт регистра 136	Старший байт регистра 137	Младший Байт регистра 137	Контрольная сумма	
11	10	00	87	00 02	04	00	0A	01	02	CRC16	CRC16

Ответ.

Нормальное ответное сообщение возвращает адрес SL, функцию, адрес первого регистра и количество записанных регистров.

Таблица 27

Адрес	Функция	Старший байт адрес первого регистра	Младший байт адреса первого регистра	Количество регистров	Контрольная сумма	
11	10	00	87	00 02	CRC16	CRC16

3.9. Функция 17: чтение информации об адресуемом устройстве**Запрос.**

Пример запроса прибору с адресом 17.

Таблица 28

Адрес	Функция	Контрольная сумма	
11	11	CRC16	CRC16

Ответ.

Общая форма ответного сообщения приведена ниже.

Таблица 29

Адрес	Функция	Число байт в поле данных	Поле данных	Контрольная сумма
-------	---------	--------------------------	-------------	-------------------

Информация в поле данных различна для каждого конкретного прибора и указана в протоколе на прибор.

Для приборов фирмы «ТЕСС-Инжиниринг» в поле данных обязательно передается следующая информация:

Таблица 30

Название параметра	Формат
Производитель прибора	ASCII строка, завершающаяся нулем : "TESS-Engineering"
Название прибора и версия ПО	ASCII строка, завершающаяся нулем, например: "URG2KM04.15.01.01"
Серийный номер	ASCII строка, завершающаяся нулем в формате "00000".

В случае, если какая-либо из строк в приборе не существует, то на ее месте в ответном сообщении должен передаваться нуль.

Остальная информация зависит от типа прибора и указывается в описании протокола прибора

3.10 Пользовательская функция 65, 66, 67, 68: чтение архива**Запрос.**

В запросе указывается адрес SL, номер функции и дата требуемой записи в формате: минута, час, день, месяц, год (0-99). Пример запроса часовой архивной записи за 12 час 10.07.03 прибора с адресом 17 :

Таблица 31

Адрес	Функция	Мин	Час	День	Месяц	Год	Контрольная сумма	
11	41	00	0С	0А	07	03	CRC16	CRC16

Ответ.

Общая форма ответного сообщения приведена ниже.

Таблица 32

Адрес	Функция	Число байт в поле данных	Поле данных	Контрольная сумма
11	41	50	Поле данных	Контрольная сумма

Информация в поле данных соответствует таблице 33:

Структура архивной записи в приборе СТУ-1:

```

struct SARoot
{
float V[6];
unsigned int T[4];
unsigned int P[4];
unsigned int FCheck;
unsigned int TFCheck;
unsigned int CheckCnt;
unsigned char Tx;
unsigned char Dummy;
float M[6];
float E[2];
};

```

Таблица 33

6 значений объемов, накопленные за период архивации V1, V2, V3, V4, V5, V6	м ³	float
4 среднеарифметических значений температур T1, T2, T3, T4	°С	
4 среднеарифметических значений давлений P1, P2, P3, P4	МПа	
Младшее слово регистра нештатных состояний		int
Старшее слово регистра нештатных состояний		int
Длительность НС, кол-во интервалов по 30 сек.		int
Значение температуры холодной воды,	°С	byte (Tx)
Значение температуры окружающей среды		byte (Ta)
6 значений масс, накопленных за период архивации, Gm1, Gm2, Gm3, Gm4, Gm5, Gm6	т	float
2 значения накопленной энергии	ГДж	float

Функции чтения архива:

- 65 - часовой архив (запись происходит каждый час на 0 минуте)
- 66 - суточный архив (запись происходит каждые сутки в час начала отсчета)
- 67 - месячный архив (запись происходит каждый месяц в день и в час начала отсчета)
- 68 - двухминутный архив (запись идет каждые две минуты при условии что двухминутный архив разрешен в приборе)

В режиме 2-х минутной архивации вместо накопленных объема, массы и энергии запоминаются среднеарифметические значения объема, массы и энергии за две минуты.

Температура холодной воды хранится в одном байте и может принимать значения от 0 до 255, соотв. от 0 °С до 25,5 °С.

В случае нахождения прибора в обесточенном состоянии более периода архивации в соответствующую архивную ячейку в параметр V1 прописывается значение 0xFFFFFFFF.

Начиная с версии 2.039 дата и время архивной записи указывают на начало диапазона архивной записи.