ОАО «ГМС Ливгидромаш»
303851 Россия, Орловская область, г. Ливны, ул. Мира, 231
тел. : +7(48677) 7-12-00, 7-69-54, 7-12-40
факс : +7(48677) 7-12-48, 7-33-49, 7-28-92
e-mail : info@hms-livgidromash.ru
www.hms-livgidromash.ru www.hms.ru

УСТРОЙСТВО УПРАВЛЕНИЯ И ЗАЩИТЫ «L4»
012.44.00.00.00

Описание протокола «MODBUS RTU»
(версия 1.1)

г. Ливны, 2015 г.

Содержание:

1. О документе

1.1 Содержание документа

Документ описывает реализацию протокола Modbus RTU в устройствах управления и защиты насосных агрегатов серии L4 (далее по тексту - контроллер) производства ОАО «ГМС Ливгидромаш». Содержится вся необходимая информация для программистов при подключении контроллеров к SCADA системам или при создании распределенных систем автоматики.

1.2 Ссылки

Данный документ ссылается на следующие документы:

1. Modbus Application Protocol Specification v1.1a (www.modbus.org)
2. Modbus messaging on TCP/IP implementation Guide Rev 1.0 (www.modbus.org)
3. Modbus over Serial Line Specification & Implementation guide V1.0 (www.modbus.org)

1.3 Термины и сокращения

RS-232 – стандарт EIA/TIA-232;
RS-485 – стандарт EIA/TIA-485 Standard.

2. Описание реализации

2.1 Интерфейс

Контроллер имеет последовательные интерфейсы RS-485 и/или RS-232. Для организации сети из двух и более приборов можно использовать преобразователь интерфейсов 232/485. Интерфейс RS-485 позволяет объединить в сеть до 128 устройств на линии длиной до 1200 м. Контроллер является ведомым (slave) устройством, отвечающим на команды с соответствующим адресом в пакете протокола.

По последовательным интерфейсам поддерживается протокол верхнего уровня Modbus с форматом пакета RTU в полном соответствии с документом «Modbus over Serial Line Specification & Implementation guide V1.0». Поддерживаются скорости передачи от 2400 бит/с до 57600 бит/с без контроля четности, 8 бит данных, 1 стоп-бит. Физический интерфейс, скорость соединения и сетевой адрес задаются при программировании контроллера. Максимальное время ожидания ответа составляет не более 100 мс.

2.2 Адреса устройств Modbus

Все устройства серии поддерживают команды Modbus в полном соответствии с синтаксисом запроса и ответа, определенным в документе «Modbus Application Protocol Specification v1.1a». Поддерживаются запросы к конкретным устройствам по их адресам, широковещательный режим не поддерживается. Адрес устройства может быть от 01h до F7h. Диапазон адресов F8h-FFh зарезервирован в стандарте Modbus.

2.3 Команды

Микроконтроллер поддерживает следующие команды:

- **03h** Чтение регистров (Read Holding Registers)
- **04h** Чтение входных регистров (Read Input Register)
- **06h** Запись регистра (Write Single Register)

Наличие команд 01h, 02h, 05h, 07h, 08h, 10h, 0Bh, 0Ch, 0Fh, 11h, 14h, 15h, 16h, 17h, 18h не обязательна. Поддержка конкретным устройством команды из приведенного выше списка отражается отдельно.

2.4 Модель данных

Спецификация Modbus определяет два типа данных, а именно биты и слова (16 бит). Каждое устройство Modbus содержит по два массива данных каждого типа, один только для чтения, другой для чтения и записи. Каждый из четырех массивов данных доступен по разным командам и имеет собственную адресацию данных.

Одни и те же данные внутри памяти устройства могут быть доступны по разным адресам в различных массивах данных. Например, байт данных, лежащий во внутренней памяти устройства, может быть доступен как восемь битовых переменных, как регистр входов и как регистр переменных. При этом в массиве данных байт данных может быть представлен несколько раз.

2.5 Адресация

Адреса запрашиваемых регистров и битов по протоколу Modbus и адреса в памяти устройства имеют однозначное табличное соответствие, но не совпадают. Таблица соответствия адресов задается программистом и должна быть отражена в документации к устройству. По одному интерфейсу может быть доступно не более 32767 байт адресуемых регистров переменных, 32767 байт регистров входов и 8192 байт, доступных через битовых переменные.

Основным способом передачи данных по протоколу Modbus является чтение или запись регистров. Реализация протокола поддерживает как побайтную адресацию, так и пословную.

Адресация битовых массивов данных полностью соответствует стандарту Modbus. Максимально возможное количество битов, передаваемых в одном пакете, не может быть более 256.

3. Описание регистров.

3.1 Регистры задания параметров объекта (Holding Register).

Чтение регистров производится командой **03 (Read Holding Register)**.

Данная функция позволяет получить двоичное содержимое 16-ти разрядных регистров адресуемого контроллера. Адресация позволяет получить за каждый запрос до 120 регистров. Регистры нумеруются с нуля. Широковещательный режим не допускается.

Адресуемый контроллер 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.

Адрес	Название		Диапазон допустимых значений		
			Тип переменной	Диапазон значений	Реальное значение
00 00	Резерв				
00 01	Режим работы		0 - автомат по датчикам уровня dL и dH, 1 - автомат по таймеру и dL(dH), 2 - по линии связи (RS-485/RS-232), 3 - управление по каналу GSM (sms)		
00 02	Функция станции		0 - налив, 1 - дренаж		
00 03	Максимальное давление, бар (метров)		int	10:4000	0,10:40,00
00 04	Минимальное давление, бар (метров)			10:4000	0,10:40,00
00 05	Время работы насоса по таймеру, минут		char	1:180	
00 06	Задержка пуска после подачи питания, секунд			0:180	
00 07	Таймер аварийного отключения, минут			0:240	
00 08	Таймер задержки включения, секунд			0:180	
00 09	Таймер задержки отключения, секунд			0:180	
00 0A	Секунды	Часы реального времени	char	0:59	
00 0B	Минуты			0:59	
00 0C	Часы			0:23	
00 0D	Дата			1:31	
00 0E	Месяц			1:12	
00 0F	Год		int	2013 : 2050	
00 10	Коррекция хода часов реального времени за 10 суток, секунд		char	-100 : +100	
00 11	Сброс пользовательских моточасов		20 - сброс моточасов		
00 12	Сброс пользовательского счетчика количества запусков двигателя		25 - сброс счетчика		
00 13	Установка заводских значений		50 - сброс на заводские уставки		
00 14	Тип датчиков уровня		0 – ЭКМ III, 1 – ЭКМ IV, 2 – ЭКМ V, 3 – ЭКМ VI, 4 - одиночные датчики уровня, 5 - аналоговый датчик давления		
00 15	Тип сигнала аналогового датчика		0 – (0...20мА), 1 – (4...20мА)		
00 16	Диапазон датчика давления, бар (метров)		int	100 : 4000	1,00 : 40,00

00 17	Тип датчика «сухого» хода	0 - реле давления (уровня), 1 - реле перепада давлений, 2 - два датчика уровня dS1 и dS2		
00 18	Диапазон трансформатора тока	int	50 : 3000	5,0 : 300,0
00 19	Проверка термодатчика	1 - да, 0 – нет		
00 1A	Тип термодатчика	0 - тип PTC, 1 – Pt100, 2 - н.з. термоконтакт		
00 1B	Проверка замыкания на корпус	1 - да, 0 – нет		
00 1C	Разрешить запуск по внешнему сигналу	1 - да, 0 – нет		
00 1D	Разрешить вход внешней ошибки	1 - да, 0 – нет		
00 1E	Использование охранной сигнализации	1 - да, 0 – нет		
00 1F	Функция универсального реле 1	0 - работа, 1 - авария, 2 - двигатель вкл/откл, 3 - внешняя ошибка, 4 - внешний пуск, 5 – замыкание dH, 6 - замыкание dL, 7 - замыкание dS1, 8 - замыкание dS2, 9 - предаварийная ситуация, 10 - срабатывание охранной сигнализации		
00 20	Функция универсального реле 2			
00 21	Параметры токового выхода	0 - (0…20мА), 1- (4…20 mA)		
00 22	Выводимое значение токового выхода	0 - ток фазы A, 1 - ток фазы B, 2 - ток фазы C, 3 - средний ток по фазам, 4 - напряжение фазы A, 5 - напряжение фазы B, 6 - напряжение фазы C, 7 - среднее значение напряжения по фазам, 8 – давление аналогового датчика		
00 23	Максимальный ток, А «Предупреждение»	int	5 : 3000	0,5 : 300,0
00 24	Максимальный ток, А «Блокировка»		5 : 3000	0,5 : 300,0
00 25	Минимальный ток, А «Предупреждение»		0 : 3000	0,0 : 300,0
00 26	Минимальный ток, А «Блокировка»		0 : 3000	0,0 : 300,0
00 27	Значение перекоса фаз по току в %	char	0 : 20	
00 28	Максимальное напряжение, В «Предупреждение»	int	2300 : 2700	230,0 : 270,0
00 29	Максимальное напряжение, В «Блокировка»		2300 : 2700	230,0 : 270,0
00 2A	Минимальное напряжение, В «Предупреждение»		1600 : 2000	160,0 : 200,0
00 2B	Минимальное напряжение, В «Блокировка»		1600 : 2000	160,0 : 200,0
00 2C	Значение перекоса фаз по напряжению, В		0 : 300	0,0 : 30,0
00 2D	Температура, ^{0}C «Предупреждение»		500 : 2000	50,0 : 200,0
00 2E	Температура, ^{0}C «Блокировка»		500 : 2000	50,0 : 200,0
00 2F	Кол-во пусков в час «Предупреждение»	char	0...100 (0 - отключает проверку)	
00 30	Кол-во пусков в час «Блокировка»		0...100 (0 - отключает проверку)	
00 31	Время блокировки пускового тока, секунд	char	1 : 60	
00 32	Время срабатывания ошибки, секунд		1 : 15	
00 33	Время выдержки после ошибки, минут		1 : 60	
00 34	Время срабатывания датчика «сухого» хода, секунд		1 : 30	
00 35	Время выдержки после «сухого» хода, минут		1 : 60	
00 36	Блокировка включения после перегрузки	0 - нет, 1 – да		
00 37	Задействовать связь с ПК (ПЛК)	0 - нет, 1 – да		
00 38	Порт линии связи с ПК (ПЛК)	0 - RS-232, 1 - RS-485		

00 39	Скорость передачи		0 - 2400, 1 - 4800, 2 - 9600, 3- 14400, 4 - 19200, 5 – 38400, 6 - 56000, 7 - 57600	
00 3A	Адрес устройства в сети		char	1 : 247
00 3B	Максимальный сетевой таймаут (связь с ПК), секунд		int	0 : 600
00 3C	Действие при таймауте соединения с ПК (ПЛК)		0 - ничего не предпринимать, 1 - авария	
00 3D	Задействовать GSM		0 - нет, 1 – да	
00 3E	Порт линии связи с GSM-модемом		0 - RS232, 1 - RS485	
00 3F	Скорость передачи		0 - 2400, 1 - 4800, 2 - 9600, 3- 14400, 4 - 19200, 5 – 38400, 6 - 56000, 7 - 57600	
00 40	Задействовать передачу sms при авариях		0 - нет, 1 – да	
00 41	Максимальный сетевой таймаут для управления по GSM (sms), минут		int	0 : 360
00 42	Действие при таймауте соединений (управление по GSM)		0 - ничего не предпринимать, 1 - авария	
00 43	D0	Номер телефона для отправки sms при авариях (без кода государства)	10 цифр, 0…9 Формат номера : +7(xxx)xxx-xx-xx Код государства: (+7) Россия	
00 44	D1			
00 45	D2			
00 46	D3			
00 47	D4			
00 48	D5			
00 49	D6			
00 4A	D7			
00 4B	D8			
00 4C	D9			
00 4D	N0	Идентификационное имя станции при отправке sms	10 символов типа char (0x20…0xFF), соответствует кодировке UNICODE 16 Bit	
00 4E	N1			
00 4F	N2			
00 50	N3			
00 51	N4			
00 52	N5			
00 53	N6			
00 54	N7			
00 55	N8			
00 56	N9			
00 57	Архивация данных (запись на карту памяти SD)		1 – разрешить архивацию, 0 - запретить	
00 58	Интервал времени для перезаписи, секунд		int	1 : 600
00 59	Действие при заполнении карты памяти		0 - остановка записи, 1 - перезапись ранних файлов	

Запись в регистры производится командой **06 (Write Single Register)**

В случае успешного выполнения функции ответное сообщение идентично запросу.

При попытке записи значений вне допустимого диапазона, буден записано минимальное или максимальное значение этого диапазона.

Чтение 2 регистров с адреса 00 00.

Запрос:

Адрес	Функция	Нач. адрес ст.	Нач. адрес мл.	Кол-во регистров ст.	Кол-во регистров мл.	CRC Lo	CRC Hi
01	03	00	00	00	02	C4	0B

Ответ:

Адрес	Функция	Счетчик байт	Данные регистра 0000 ст.	Данные регистра 0000 мл.	Данные регистра 0001 ст.	Данные регистра 0001 мл.	CRC Lo	CRC Hi
01	03	04	00	05	00	01	2B	F2

Запись регистра по адресу 00 08.

Запрос:

Адрес	Функция	Нач. адрес ст.	Нач. адрес мл.	Данные регистра 0008 ст.	Данные регистра 0008 мл.	CRC Lo	CRC Hi
01	06	00	08	00	14	08	07

Ответ:

Адрес	Функция	Нач. адрес ст.	Нач. адрес мл.	Данные регистра 0008 ст.	Данные регистра 0008 мл.	CRC Lo	CRC Hi
01	06	00	08	00	14	08	07

Нормальный ответ контроллера повторяет запрос.

3.2 Регистры чтения параметров объекта (Input Register).

Чтение регистров производится командой **04 (Read Input Register)**.

Данная функция позволяет получить двоичное содержимое 16-ти разрядных регистров адресуемого контроллера. Адресация позволяет получить за каждый запрос до 120 регистров. Регистры нумеруются с нуля.

Широковещательный режим не допускается.

Адресуемый контроллер 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.

С адреса 012Ah находится журнал ошибок станции. Количество записей – 20 (20*18 = 360 регистров, 720 байт данных).

Запись содержит поля: код ошибки, дата, месяц, год, час, мин, значения токов, напряжений и температуры на момент аварии и время сброса ошибки (нули, если ошибка еще не сброшена).

Записи располагаются в хронологическом порядке, начиная с последней по времени ошибки. При возникновении очередной ошибки происходит сдвиг вниз на одну запись. Последняя ошибка всегда находится в первой записи.

Адрес	**Название**	**Описание**		
01 00	Управление (чтение и запись)	бит		
		0	Реле “ Двигатель ”	1: Вкл, 0: Откл
		1	Реле “Авария”	1: Включено
		2	Реле универсальное 1	1: Включено
		3	Реле универсальное 2	1: Включено
		4	Сброс ошибки станции	1: команда сброса
		5	Сброс контроллера	1: команда сброса
		6	Постановка на охрану	1: команда постановки
		7	Снятие с охраны	1: команда снятия
		8-F	Резерв	

<table>
<tr><th>Адрес</th><th>Название</th><th>Описание</th></tr>
<tr><td>01 01</td><td>Состояние станции
(только чтение)</td><td>0: Работа станции приостановлена
1: Проверка перед запуском
2: Запуск двигателя
3: Ожидание замыкания входа «Внешнее управление»
4: Ожидание нажатия кнопки «ПУСК»
5: Ожидание нажатия кнопки «СТОП»
6: Ожидание верхнего уровня
7: Ожидание нижнего уровня
8: Ожидание размыкания входа dL (Режим – По таймеру)
9: Ожидание замыкания входа dH (Режим – По таймеру)
10: Двигатель включен на время работы по таймеру
11: Задержка пуска
12: Задержка останова
13: Двигатель включен сигналом «Внешнее управление»
14: Задержка пуска после подачи питания
15: Ожидание включения (по линии связи)
16: Ожидание отключения (по линии связи)
17: Ожидание команды включения из SMS
18: Ожидание команды отключения из SMS
19: Диагностика
20: Ожидание наполнения скважины до датчика dS2</td></tr>
<tr><td>01 02</td><td>Состояние охранной сигнализации</td><td>0: отключена в установочном меню
1: поставлена на охрану
2: ожидание замыкания датчика двери
3: несанкционированный доступ
4: снята с охраны</td></tr>
<tr><td>01 03</td><td>Состояние GSM-модема</td><td>0: GSM-модем не найден
1: идет инициализация модема
2: ошибка SIM-карты
3: ошибка ввода PIN-кода
4: ошибка инициализации модема
5: ошибка регистрации в сети
6: поиск сети
7: зарегистрирован в сети (домашняя)
8: зарегистрирован в сети (роуминг)
9: отправка SMS
10: SMS успешно отправлено
11: ошибка отправки SMS</td></tr>
<tr><td>01 04</td><td>Дискретные входы</td><td>
<table>
<tr><th>бит</th><th></th><th></th></tr>
<tr><td>0</td><td>Датчик верхнего уровня (dH)</td><td rowspan="7">1: замкнут
0: разомкнут</td></tr>
<tr><td>1</td><td>Датчик нижнего уровня (dL)</td></tr>
<tr><td>2</td><td>Датчик “сухого” хода 1 (dS1)</td></tr>
<tr><td>3</td><td>Датчик “сухого” хода 2(dS2)</td></tr>
<tr><td>4</td><td>Внешнее управление (E.Run)</td></tr>
<tr><td>5</td><td>Внешняя ошибка (E.Error)</td></tr>
<tr><td>6</td><td>Датчик двери охранной сигнализации (Alarm)</td></tr>
<tr><td>7</td><td>Переключатель режима работы «Ручной/Автомат» (Auto)</td><td>1: замкнут, “Автомат”
0: разомкнут, “Ручной”</td></tr>
<tr><td>8</td><td>Замыкание на корпус (M_FA)</td><td>0: нет,
1: замыкание</td></tr>
<tr><td>9-F</td><td>Резерв</td><td></td></tr>
</table>
</td></tr>
</table>

Адрес	Название	Диапазон допустимых значений		
		Тип переменной	**Диапазон значений**	**Реальное значение**
01 05	Код аварии	0: Нет аварии 1: Неправильное чередование фаз 2: Повышение напряжения 3: Понижение напряжения 4: Перекос по напряжению 5: Повышение тока 6: Понижение тока 7: Перекос по току 8: «Сухой» ход 9: Внешняя ошибка 10: Неправильное срабатывание д. у. 11: Таймер аварийного отключения 12: Замыкание (утечка) на корпус 13: Внутренняя ошибка L4 14: Превышение количества пусков в час 15: Отказ аналогового датчика давления 16: Таймаут соединения с ПК (ПЛК) 17: Таймаут соединения GSM 18: Перегрев двигателя		
01 06	Оставшееся время выдержки при аварии в секундах	int	0 : 3600	
01 07	Код предупреждения 1	0: Нет предупреждения 1: Максимальный ток 2: Минимальный ток 3: Максимальное напряжение 4: Минимальное напряжение 5: Температура двигателя 6: Превышение количества пусков в час 7: Несанкционированный доступ 8: Ошибка при работе с SD-картой		
01 08	Код предупреждения 2			
01 09	Код предупреждения 3			
01 0A	Код предупреждения 4			
01 0B	Код предупреждения 5			
01 0C	Код предупреждения 6			
01 0D	Напряжение фазы A(L1), В	int	0 : 3000	0,0 : 300,0
01 0E	Напряжение фазы B(L2), В			
01 0F	Напряжение фазы C(L3), В			
01 10	Среднее напряжение по фазам, В			
01 11	Перекос по напряжению, %		0 : 1000	0,0 : 100,0
01 12	Ток фазы A(L1), А		0 : 3000	0,0 : 300,0
01 13	Ток фазы B(L2), А			
01 14	Ток фазы C(L3), А			
01 15	Средний ток по фазам, А			
01 16	Перекос по току, %		0 : 1000	0,0 : 100,0
01 17	Состояние термодатчика	0 - исправен, 1 - обрыв, 2 - к.з., 3 – перегрев, 4 - замкнут, 5 – разомкнут, 6 – не используется		
01 18	Температура двигателя, ^{0}C (только для Pt 100)	int	-700 : +3000 0x7FFF - нет значений	-70,0…+300,0
01 19	Состояние аналогового датчика давления 0…20mA(4…20mA)	0 - исправен, 1 - обрыв, 2 - к.з.		
01 1A	Давление, бар (метров)	int	0 : 4000	0,00 : 40,00
01 1B	Давление, в mA		0 : 2500	0,00 : 25,00
01 1C	Время работы по таймеру (сколько прошло) в секундах	int	0 : 20000	

01 1D	Время работы по таймеру (сколько осталось) в секундах		0 : 20000	
01 1E	Время наработки двигателя (сбрасываемое), часов	int	0…0xFFFF (0…65535)	
01 1F	Кол-во пусков двигателя (сбрасываемое)	int	0…0xFFFF (0…65535)	
01 20	Время наработки двигателя общее, часов	int	0…0xFFFF (0…65535)	
01 21	Кол-во пусков двигателя общее	int	0…0xFFFF (0…65535)	
01 22	Температура шкафа (контроллера) ^{0}C	int	-400 : +1000 0x7FFF - нет значений	-40,0…+100,0
01 23	Значение на токовом выходе	int	0…0xFFFF (0…65535)	
01 24	Резерв			
01 25	Резерв			
01 26	Резерв			
01 27	Резерв			
01 28	Резерв			
01 29	Резерв			

Журнал аварий, 20 записей, 20*18 = 360 регистров, 720 байт данных.

Адрес	**Название**		**Диапазон допустимых значений**		
			Тип переменной	**Диапазон значений**	**Реальное значение**
Dec (Hex)					
298 (012A)	Код ошибки	0 – пустая запись	char	0 : 20	
299 (012B)	Дата	Время возникновения аварии (0 – пустая запись)		1:31	
300 (012C)	Месяц			1:12	
301 (012D)	Год		int	2013 : 2050	
302 (012E)	Час		char	0:23	
303 (012F)	Мин			0:59	
304 (0130)	Ток фазы A(L1), A		int	0 : 3000	0,0 : 300,0
305 (0131)	Ток фазы B(L2), A				
306 (0132)	Ток фазы C(L3), A				
307 (0133)	Напряжение фазы A(L1), B				
308 (0134)	Напряжение фазы B(L2), B				
309 (0135)	Напряжение фазы C(L3), B				
310 (0136)	Температура, ^{0}C (только для Pt 100)		int	-700 : +3000 0x7FFF - нет значений	-70,0…+300,0
311 (0137)	Дата	Время сброса аварии (0 – авария пока не сброшена)	char	1 : 31	
312 (0138)	Месяц			1 : 12	
313 (0139)	Год		int	2013 : 2050	
314 (013A)	Час		char	0 : 23	
315 (013B)	Мин			0 : 59	

316-333 (013C-014D)	Запись №2			
334-351 (014E-015F)	Запись №3			
352-369 (0160-0171)	Запись №4			
370-387 (0172-0183)	Запись №5			
388-405 (0184-0195)	Запись №6			
406-423 (0196-01A7)	Запись №7			
424-441 (01A8-01B9)	Запись №8			
442-459 (01BA-01CB)	Запись №9			
460-477 (01CC-01DD)	Запись №10			
478-495 (01DE-01EF)	Запись №11			
496-513 (01F0-0201)	Запись №12			
514-531 (0202-0213)	Запись №13			
532-549 (0214-0225)	Запись №14			
550-567 (0226-0237)	Запись №15			
568-585 (0238-0249)	Запись №16			
586-603 (024A-025B)	Запись №17			
604-621 (025C-026D)	Запись №18			
622-639 (026E-027F)	Запись №19			
640-657 (0280-0291)	Запись №20			

Чтение 4 регистров с адреса 00 09.

Запрос	Ответ
01 – Адрес 04 - Функция 00 - Начальный адрес ст. 09 - Начальный адрес мл. 00 - Количество регистров ст. 04 - Количество регистров мл. 21 – CRC Lo CB- CRC Hi	01 - Адрес 04 - Функция 08 - Счетчик байт 00 - Данные регистра 00 09 ст. 00 - Данные регистра 00 09 мл. 00 - Данные регистра 00 0A ст. 00 - Данные регистра 00 0A мл. 00 - Данные регистра 00 0B ст. 00 - Данные регистра 00 0B мл. 01 - данные регистра 00 0C ст. 00 - Данные регистра 00 0C мл. 25 - CRC Lo 9D- CRC Hi

4. Исключительные ситуации

Микроконтроллер поддерживает сообщения информирования клиента (мастера) Modbus об исключительных ситуациях (Exception). Формат возвращаемых пакетов полностью соответствует документу «Modbus Application Protocol Specification v1.1a». Сообщения об исключительных ситуациях возникают только на запросы, адресованные данному устройству с правильным значением CRC пакета.

Код ошибки	Название	Описание
01	Неподдерживаемая команда	Возникает только при запросе с номером команды, которую не поддерживает данное устройство.
02	Неподдерживаемый адрес данных	Возникает только при запросе с адресом данных, которых нет в таблицах соответствия между адресами Modbus и внутренней памятью устройства
03	Неверное количество данных	В запросе содержится значения недопустимые для сервера. Например, запрос количества регистров более чем 120.

Когда контроллер обнаруживает одну их этих ошибок, он посылает ответное сообщение, содержащее адрес, 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.

Адрес	Функция	Старший байт адреса	Младший байт адреса	Старший байт числа ячеек	Младший байт числа ячеек	CRC
01	03	00	12	00	06	xx xx

Этот запрос требует от контроллера с адресом 01 данных 6 регистров с адреса 18. Но, например, этот контроллер имеет максимальный адрес 0x0016, а запрашиваемое количество данных превышает диапазон адреса и является ошибочным. Соответственно, будет сгенерировано следующее ответное сообщение.

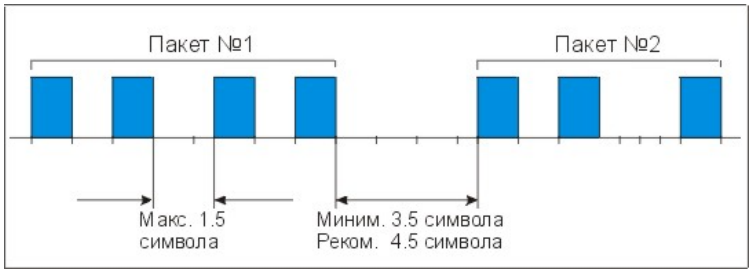
Адрес	Функция	Код исключительной ситуации	CRC
01	83	03	xx xx

Значение в поле функции равно оригинальному значению с установленным в единицу старшим битом. Код исключительной ситуации 03 указывает на ошибочное количество данных.

5. Задержки между пакетами

Временные задержки между пакетами и символами пакетов полностью соответствуют «Modbus over Serial Line Specification & Implementation guideV1.0». Между символами одного пакета может быть задержка длинной не
более полутора символов. Между пакетами должна быть задержка не менее 3,5 символов. Рекомендуется начать передавать следующий пакет не ранее чем через 4,5 символа после получения последнего бита предыдущего пакета. Если в интервале между 1,5 символами и 3,5 символами после прихода последнего символа, приходит первый символ следующего пакета, сбрасываются оба пакета.

Комментарий: задержка длинной в символ - это время необходимое, для того чтобы передать 8 бит данных при данной скорости передачи и параметрах соединения.



5.1 Рекомендуемые задержки между пакетами

Скорость интерфейса при параметрах 8N1	Минимальное время между символами в пакете	Минимальная задержка между пакетами	Рекомендуемая задержка между пакетами
2400Кбит/с	6,3мс	14,6мс	18,8мс
4800Кбит/с	3,2мс	7,3мс	9,4мс
9600 Кбит/с	1,6мс	3,6мс	4,7мс
14400Кбит/с	1,0мс	2,4мс	3,1мс
19200Кбит/с	0,8мс	1,8мс	2,3мс

6 Генерация CRC

CRC это 16-ти разрядная величина, т.е. два байта. CRC вычисляется передающим устройством и добавляется к сообщению. Принимающее устройство также вычисляет CRC в процессе приема и сравнивает вычисленную величину с полем контрольной суммы пришедшего сообщения. Если суммы не совпали - то имеет место ошибка.

16-ти битовый регистр CRC предварительно загружается числом FFFF hex. Процесс начинается с добавления байтов сообщения к текущему содержимому регистра. Для генерации CRC используются только 8 бит данных. Старт и стоп биты, бит паритета, если он используется, не учитываются в CRC.

В процессе генерации CRC, каждый 8-ми битовый символ складывается по ИСКЛЮЧАЮЩЕМУ ИЛИ с содержимым регистра. Результата сдвигается в направлении младшего бита, с заполнением 0 старшего бита. Младший бит извлекается и проверяется. Если младший бит равен 1, то содержимое регистра складывается с определенной ранее, фиксированной величиной, по ИСКЛЮЧАЮЩЕМУ ИЛИ. Если младший бит равен 0, то ИСКЛЮЧАЮЩЕЕ ИЛИ не делается.

Этот процесс повторяется, пока не будет сделано 8 сдвигов. После последнего (восьмого) сдвига, следующий байт складывается с содержимым регистра и процесс повторяется снова. Финальное содержание регистра, после обработки всех байтов сообщения и есть контрольная сумма CRC.

6.1 Алгоритм генерации CRC:

1. 16-ти битовый регистр загружается числом FFFFh (все 1), и используется далее как регистр CRC.
2. Первый байт сообщения складывается по ИСКЛЮЧАЮЩЕМУ ИЛИ с содержимым регистра CRC. Результат помещается в регистр CRC.
3. Регистр CRC сдвигается вправо (в направлении младшего бита) на 1 бит, старший бит заполняется нулем.
4. (Если младший бит 0): Повторяется шаг 3 (сдвиг)
   (Если младший бит 1): Делается операция ИСКЛЮЧАЮЩЕЕ ИЛИ регистра CRC и полиномиального числа A001 hex.
5. Шаги 3 и 4 повторяются восемь раз.
6. Повторяются шаги со 2 по 5 для следующего сообщения. Это повторяется до тех пор пока все байты сообщения не будут обработаны.
7. Финальное содержание регистра CRC и есть контрольная сумма.

6.2 Размещение CRC в сообщении

При передаче 16 бит контрольной суммы CRC в сообщении, сначала передается младший байт, затем старший. Например, если CRC равна 1288 hex:

Адрес	Функция	Счетчик байт	Данные	Данные	Данные	Данные	CRC Lo	CRC Hi
							88	**12**

6.3 Пример функции на языке С, реализующей генерацию CRC

```
void main (void)
{
unsigned char CRC_Hi, CRC_Lo;          // Старший и младший байты контрольной суммы
unsigned char Send_Otvet[128];         // Массив данных, содержащий ответ
        …
        …
        // В массиве Send_Otvet[] содержатся 8 байт ответного сообщения
        Create_CRC(8);
        // Добавляем к массиву Send_Otvet[] 9 и 10 байты контрольной суммы (CRC_Lo и CRC_Hi)
        Send_Otvet[9]= CRC_Lo;
        Send_Otvet[10]= CRC_Hi;
        // Отправляем ответ
        …
}// End



void Create_CRC (unsigned char Kol_Bytes)      // Подсчет CRC по количеству байт массива Send_Otvet[]
{
unsigned int Register = 0xFFFF;
unsigned int Lsb;
unsigned char i, j;

      for (i=0; i<Kol_Bytes; i++)
      {
            Register^=Send_Otvet[i];
            for ( j=0; j<8; j++)
            {
                  Lsb = Register & 0x0001;
                  Register = Register >> 1;        //  Сдвигаем на 1 вправо
                  if (Lsb) Register^=0xA001;       // Если младший бит 0, то исключающее ИЛИ с числом 0xA001
            }
      }
      CRC_Hi = Register >> 8;
      CRC_Lo = Register;

}// End
```