Виктор Денисенко

Протоколы и сети Modbus и Modbus TCP

Modbus: общие положения

Протокол Modbus и одноимённая сеть [1-4] являются самыми распространёнными в мире среди протоколов и сетей. Несмотря на свой возраст (Modbus стал стандартом де-факто ещё в 1979 году) он не только не устарел, но, наоборот, демонстрирует существенно возросшее количество ориентированных на него новых разработок и увеличивающийся объём организационной поддержки протокола. Миллионы Modbus-устройств по всему миру продолжают успешно работать, обновляются версии описания протокола [2].

Одним из главных преимуществ Modbus является отсутствие необходимости в специальных интерфейсных контроллерах (PROFIBUS и CAN требуют для своей реализации заказных микросхем), также к преимуществам следует причислить простоту программной реализации и элегантность принципов функционирования. Всё это снижает затраты на освоение стандарта как системными интеграторами, так и разработчиками контроллерного оборудования. Высокая степень открытости протокола обеспечивается полностью бесплатными текстами стандартов, которые можно скачать с сайта www.modbus.org.

В России Modbus по распространённости конкурирует только с PROFIBUS. Популярность протокола в настоящее время объясняется, прежде всего, совместимостью с большим количеством оборудования, которое поддерживает протокол Modbus. Кроме того, Modbus имеет высокую достоверность передачи данных, связанную с применением надёжного метода контроля ошибок. Modbus позволяет унифицировать команды обмена благодаря стандартизации номеров (адресов) регистров и функций их чтения-записи.

Основным недостатком Modbus является сетевой обмен по типу «ведущий–ведомый», что не позволяет ведомым устройствам передавать данные по мере их появления и поэтому требует интенсивного опроса ведомых устройств ведущим.

Разновидностями Modbus выступают Modbus Plus [4], представляющий собой многомастерный протокол с кольцевой передачей маркера, и протокол Modbus TCP [5], рассчитанный на использование в сетях Ethernet и Интернет.

Протокол Modbus имеет два режима передачи: RTU (remote terminal unit – удалённое терминальное устройство) и ASCII. Стандарт предусматривает, что режим RTU в протоколе Modbus должен присутствовать обязательно, а режим ASCII является опционным. Пользователь может выбирать любой из них, но все модули, включённые в сеть Modbus, должны иметь один и тот же режим передачи.

Мы рассмотрим только протокол Modbus RTU, поскольку Modbus ASCII в России практически не используется. Отметим, что Modbus ASCII нельзя путать с частнофирменным протоколом DCON, который используется в модулях фирм Advantech и ICP DAS и не соответствует стандарту Modbus.

Стандарт Modbus предусматривает применение физического интерфейса RS-485, RS-422 или RS-232. Наиболее часто применяемым для организации промышленной сети является 2-проводной интерфейс RS-485. Для соединений точка–точка может быть использован интерфейс RS-232 или RS-422.

В стандарте Modbus имеются требования *обязательные*, *рекомендуемые* и *опционные* (необязательные). Существует три степени соответствия стандарту: полностью соответствует (когда протокол соответствует всем обязательным и всем рекомендуемым требованиям), условно соответствует (когда протокол соответствует только обязательным требованиям и не соответствует рекомендуемым) и не соответствует.

Модель OSI протокола Modbus содержит три уровня: физический, канальный и прикладной (табл. 1).

Физический уровень

В новых разработках на основе Modbus стандарт рекомендует использовать интерфейс RS-485 с двухпроводной линией передачи, но допускается применение четырёхпроводной линии и интерфейса RS-232.

Modbus-шина должна состоять из одного магистрального кабеля, от которого могут быть сделаны отводы. Магистральный кабель Modbus должен содержать 3 проводника в общем экране, два из которых представляют собой витую пару, а третий соединяет общие («земляные») выводы всех интерфейсов RS-485 в сети. Общий провод и экран должны быть заземлены *в одной точке*, желательно около ведущего устройства.

Устройства могут подключаться к кабелю тремя способами:

- непосредственно к магистральному кабелю;
- через пассивный разветвитель (тройник);
- через активный разветвитель, содержащий развязывающий повторитель интерфейса.

Таблица 1

Модель OSI для Modbus

НОМЕР УРОВНЯ	НАЗВАНИЕ УРОВНЯ	РЕАЛИЗАЦИЯ
7	Прикладной	Modbus application protocol
6	Уровень представления	Нет
5	Сеансовый	Нет
4	Транспортный	Нет
3	Сетевой	Нет
2	Канальный (передачи данных)	Протокол «ведущий–ведомый». Режимы RTU и ASCII
1	Физический	RS-485 или RS-232

В документации на устройство и на разветвитель должны быть указаны наименования подключаемых цепей.

На каждом конце магистрального кабеля должны быть установлены резисторы для согласования линии передачи, как это требуется для интерфейса RS-485. В отличие от RS-485 наличие терминальных резисторов в соответствии со стандартом Modbus является обязательным независимо от скорости обмена. Их номинал может быть равным 150 Ом при мощности 0,5 Вт. Терминальные резисторы, а также резисторы, устраняющие неопределённость состояния линии при высокоомном состоянии передатчиков, устанавливаются так же, как и в других сетях на основе физического интерфейса RS-485. Стандарт требует, чтобы в руководствах по эксплуатации устройств Modbus было сказано, имеются ли указанные резисторы внутри устройства или их необходимо устанавливать при монтаже сети. Если требуются внешние резисторы, то они должны иметь номинал в интервале от 450 до 650 Ом и быть установлены только в одном месте в пределах каждого сегмента сети (сегментами считаются части сети между повторителями интерфейса).

Modbus-устройство обязательно должно поддерживать скорости обмена 9600 и 19 200 бит/с, из них 19 200 бит/с устанавливается по умолчанию. Допускаются также скорости 1200, 2400, 4800, ... 38 400 бит/с, 65 и 115 кбит/с, ...

Скорость передачи должна выдерживаться в передатчике с погрешностью не хуже 1%, а приёмник должен принимать данные при отклонении скорости передачи до 2%.

Сегмент сети, не содержащий повторителей интерфейса, должен допускать подключение до 32 устройств, однако их количество может быть увеличено, если это допустимо исходя из нагрузочной способности передатчиков и входного сопротивления приёмников, которые должны быть приведены в документации на интерфейсы. Указание этих параметров в документации является обязательным требованием стандарта.

Максимальная длина магистрального кабеля при скорости передачи 9600 бит/с и сечении жил более 0,13 мм^2 (AWG 26) составляет 1 км. Отводы от магистрального кабеля не должны быть длиннее 20 м. При использовании многопортового пассивного разветвителя с N отводами длина каждого отвода не должна превышать значения $40/N$ м.

Modbus не устанавливает конкретных типов разъёмов, но если используются разъёмы RJ-45, mini-DIN или D-shell, они должны быть экранированными, а цоколёвки должны соответствовать стандарту.

Для минимизации ошибок при монтаже рекомендуется использовать провода следующих цветов: жёлтый – для положительного вывода RS-485 (на котором устанавливается логическая 1, когда через интерфейс выводится логическая 1), коричневый – для второго вывода интерфейса RS-485, серый – для общего провода.

Типовым сечением кабеля является AWG 24 (0,2 мм^2, диаметр провода 0,51 мм). При использовании кабеля категории 5 его длина не должна превышать 600 м. Волновое сопротивление кабеля желательно выбирать более 100 Ом, особенно для скорости обмена более 19 200 бит/с.

Канальный уровень

Протокол Modbus предполагает, что только одно ведущее устройство (контроллер) и до 247 ведомых (модулей ввода-вывода) могут быть объединены в промышленную сеть. Обмен данными всегда инициируется ведущим. Ведомые устройства никогда не начинают передачу данных, пока не получат запрос от ведущего. Также ведомые устройства не могут обмениваться данными друг с другом. Поэтому в любой момент времени в сети Modbus может происходить только один акт обмена.

Адреса с 1 по 247 являются адресами Modbus-устройств в сети, а с 248 по 255 зарезервированы. Ведущее устройство не должно иметь адреса, и в сети не должно быть двух устройств с одинаковыми адресами.

Ведущее устройство может посылать запросы всем устройствам одновременно (широковещательный режим) или только одному. Для широковещательного режима зарезервирован адрес 0 (при использовании в команде этого адреса она принимается всеми устройствами сети).

Описание кадра (фрейма) протокола Modbus

В протоколе Modbus RTU сообщение начинает восприниматься как новое после паузы (тишины) на шине длительностью не менее 3,5 шестнадцатеричных символов (14 бит), то есть величина паузы в секундах зависит от скорости передачи.

Формат кадра показан на рис. 1. Поле адреса всегда (даже в ответах на команду, посланную ведущим) содержит только адрес ведомого устройства. Благодаря этому ведущее устройство знает, от какого модуля пришёл ответ.

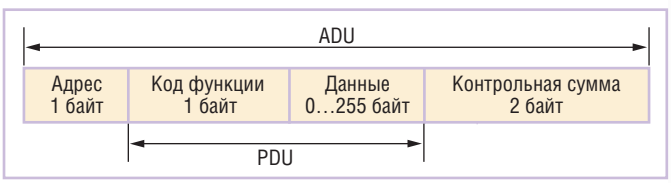

Рис. 1. Формат кадра протокола Modbus RTU:
PDU (protocol data unit) – элемент данных протокола;
ADU (application data unit) – элемент данных приложения

Поле «Код функции» говорит модулю о том, какое действие нужно выполнить.

Поле «Данные» может иметь произвольное количество байтов в диапазоне от 0 до 255. В нём может содержаться информация о параметрах, используемых в запросах контроллера или ответах модуля.

Поле «Контрольная сумма» содержит контрольную сумму CRC длиной 2 байта.

Структура данных в режиме RTU

В режиме RTU данные передаются младшими разрядами вперёд (рис. 2).

По умолчанию в режиме RTU бит паритета устанавливают равным 1, если количество двоичных единиц в байте нечётное, и равным 0, если оно чётное. Такой паритет называют чётным (even parity), а метод контроля называют контролем чётности.

При чётном количестве двоичных единиц в байте бит паритета может быть равен 1. В этом случае говорят, что паритет является нечётным (odd parity).

Стартовый бит	1 МЗР	2	3	4	5	6	7	8	Бит паритета	Стоп-бит

Рис. 2. Последовательность битов в режиме RTU
(МЗР – младший значащий разряд; при отсутствии бита паритета на его место записывается второй стоп-бит)

Таблица 2

Пример кодов Modbus RTU для модуля RealLab! типа NL-16DI

ОБОЗНАЧЕНИЕ РЕГИСТРА	HEX-АДРЕС РЕГИСТРА	ЧТО ЧИТАЕТСЯ ИЛИ ЗАПИСЫВАЕТСЯ	КОД ФУНКЦИИ ЧТЕНИЯ РЕГИСТРА	КОД ФУНКЦИИ ЗАПИСИ В РЕГИСТР	ПРИМЕЧАНИЕ
00001	00h 00h	Дискретный выход 0	01	05	1 или 0
00002	00h 01h	Дискретный выход 1	01	05	1 или 0
10001	00h 00h	Дискретный вход 0	02	–	1 или 0
10002	00h 01h	Дискретный вход 1	02	–	1 или 0
10003	00h 02h	Дискретный вход 2	02	–	1 или 0
10004	00h 03h	Дискретный вход 3	02	–	1 или 0
10005	00h 04h	Дискретный вход 4	02	–	1 или 0
10006	00h 05h	Дискретный вход 5	02	–	1 или 0
10007	00h 06h	Дискретный вход 6	02	–	1 или 0
10008	00h 07h	Дискретный вход 7	02	–	1 или 0
10009	00h 08h	Дискретный вход 8	02	–	1 или 0
10010	00h 09h	Дискретный вход 9	02	–	1 или 0
10011	00h 0Ah	Дискретный вход 10	02	–	1 или 0
10012	00h 0Bh	Дискретный вход 11	02	–	1 или 0
10013	00h 0Ch	Дискретный вход 12	02	–	1 или 0
10014	00h 0Dh	Дискретный вход 13	02	–	1 или 0
10015	00h 0Eh	Дискретный вход 14	02	–	1 или 0
10016	00h 0Fh	Дискретный вход 15	02	–	1 или 0
40201	00h C8h	Имя модуля	03	10	–
40213	00h D4h	Версия программы	03	–	–
40513	02h 00h	Адрес модуля	03	06	0001h–00F7h (допустимый диапазон значений)
40514	02h 01h	Скорость UART	03	06	0003h–000Ah (допустимый диапазон значений)
40518	02h 05h	Протокол	03	06	0000h – ASCII, 0001h – RTU
40769	03h 00h	Значение на выходе после включения питания модуля Power On Value0	03	06	0000h–0003h (допустимый диапазон значений)

Контроль чётности может отсутствовать вообще. В этом случае вместо бита паритета должен использоваться второй стоповый бит. Для обеспечения максимальной совместимости с другими продуктами рекомендуется использовать возможность замены бита паритета на второй стоповый бит.

Ведомые устройства могут воспринимать любой из вариантов: чётный, нечётный паритет или его отсутствие.

Структура сообщения Modbus RTU

Сообщения Modbus RTU передаются в виде кадров, для каждого из которых известны начало и конец. Признаком начала кадра является пауза (тишина) продолжительностью не менее 3,5 шестнадцатеричных символов (14 бит). Кадр должен передаваться непрерывно. Если при передаче кадра обнаруживается пауза продолжительностью более 1,5 шестнадцатеричных символов (6 бит), то считается, что кадр содержит ошибку и должен быть отклонён принимающим модулем. Эти величины пауз должны строго соблюдаться при скоростях ниже 19 200 бит/с, однако при более высоких скоростях рекомендуется использовать фиксированные значения паузы – 1,75 мс и 750 мкс соответственно.

Контроль ошибок

В режиме RTU имеются два уровня контроля ошибок в сообщении:

- контроль паритета для каждого байта (опционно);
- контроль кадра в целом с помощью CRC-метода.

CRC-метод используется независимо от проверки паритета. Значение CRC устанавливается в ведущем устройстве перед передачей. При приёме сообщения вычисляется код CRC для всего сообщения и сравнивается с его значением, указанным в поле CRC кадра. Если оба значения совпадают, считается, что сообщение не содержит ошибки.

Стартовые, стоповые биты и бит паритета в вычислении CRC не участвуют.

Прикладной уровень

Прикладной уровень Modbus RTU версии 1.1a описан в [3]. Он обеспечивает коммуникацию между устройствами типа «ведущий–ведомый». Прикладной уровень является независимым от физического и канального, в частности, он может использовать протоколы Ethernet TCP/IP (Modbus TCP/IP), Modbus Plus (многомастерная сеть с передачей маркера), интерфейсы RS-232, RS-422, RS-485,

оптоволоконные линии, радиоканалы и другие физические среды для передачи сигналов.

Прикладной уровень Modbus основан на запросах с помощью *кодов функций*. Код функции указывает ведомому устройству, какую операцию оно должно выполнить.

При использовании протокола прикладного уровня с различными протоколами транспортного и канального уровня сохраняется неизменным основной блок Modbus-сообщения, включающий код функции и данные (этот блок называется PDU – protocol data unit – элемент данных протокола). К блоку PDU могут добавляться дополнительные поля при использовании его в различных промышленных сетях, и тогда он называется ADU – application data unit – элемент данных приложения.

Коды функций

Стандартом Modbus предусмотрены три категории кодов функций: установленные стандартом, задаваемые пользователем и зарезервированные.

Коды функций являются числами в диапазоне от 1 до 127, причём коды в диапазоне от 65 до 72 и от 100 до 110 относятся к задаваемым пользователем функциям. Коды в диапазоне от 128 до 255 зарезервированы для пересылки кодов ошибок в ответном сообщении. Код 0 не используется.

Коды ошибок используются ведомым устройством, чтобы определить, какое действие предпринять для их обработки. Значения кодов и их смысл описаны в стандарте на Modbus RTU [3].

Поле данных (рис. 1) в сообщении, посланном от ведущего устройства ведомому, содержит дополнительную информацию, которую ведомое устройство использует, чтобы выполнить функцию, указанную в поле «Код функции». Поле данных может содержать значения состояний дискретных входов/выходов, адреса регистров, из которых надо считывать (записывать) данные, количество байтов данных, ссылки на переменные, количество переменных, код подфункций и т.п.

Если ведомое устройство нормально выполнило принятую от ведущего функцию, то в ответе поле «Код функции» содержит ту же информацию, что и в запросе. В противном случае ведомый выдаёт код ошибки. В случае ошибки код функции в ответе равен коду функции в запросе, увеличенному на 128.

Содержание поля данных

В сообщении ведущего устройства ведомому поле данных содержит дополнительную информацию, необходимую для выполнения указанной функции. Например, если код функции указывает, что необходимо считать данные из группы регистров устройства ввода (код функции 03 hex), то поле данных содержит адрес начального регистра и количество регистров. Если ведущее устройство посылает команду записи данных в группу регистров (код функции 10 hex), то поле данных должно содержать адрес начального регистра, количество регистров, количество байтов данных и данные для записи в регистр.

Конкретное содержание поля данных устанавливается стандартом для каждой функции отдельно.

В некоторых сообщениях поле данных может иметь нулевую длину.

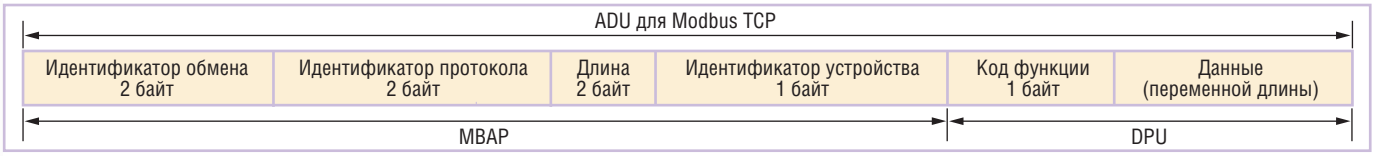

Рис. 3. Часть фрейма Modbus TCP, встраиваемая в поле «Данные» фрейма Ethernet [1]

Список кодов Modbus

В табл. 2 приведён пример кодов Modbus RTU для модуля дискретного ввода и вывода типа RealLab! NL-16DI (фирмы НИЛ АП). Для чтения логических состояний входов модуля через интерфейс RS-485 необходимо послать команду в формате, показанном на рис. 1, где в полях «Адрес» и «Код функции» указываются значения из соответствующих граф табл. 2.

Modbus TCP

Протокол Modbus TCP [5] (или Modbus TCP/IP) используется для того, чтобы подключить устройства с протоколом Modbus к Ethernet или сети Internet. Он использует кадры Modbus RTU на 7-м (прикладном) уровне модели OSI, протоколы Ethernet на 1-м и 2-м уровнях модели OSI и TCP/IP на 3-м и 4-м уровнях, то есть Ethernet TCP/IP используется для транспортировки модифицированного кадра Modbus RTU.

Кадр Modbus RTU (рис. 1) в этом случае не имеет поля контрольной суммы, поскольку используется стандартная контрольная сумма Ethernet TCP/IP; нет также поля адреса, поскольку в Ethernet используется иная систем адресации. Таким образом, только два поля – «Код функции» и «Данные» (блок PDU) встраиваются в протокол Ethernet TCP/IP. Перед ними вставляется новое поле (рис. 3) – MBAP (Modbus application protocol – прикладной протокол Modbus). Поле «Идентификатор обмена» используется для идентификации сообщения в случае, когда в пределах одного TCP-соединения клиент посылает серверу несколько сообщений без ожидания ответа после каждого сообщения. Поле «Идентификатор протокола» содержит нули и зарезервировано для будущих применений. Поле «Длина» указывает количество следующих за ним байтов. Поле «Идентификатор устройства» идентифицирует удалённый сервер, расположенный вне сети Ethernet (например, в сети Modbus RTU, которая соединена с Ethernet с помощью межсетевого моста). Чаще всего это поле содержит нули или единицы, игнорируется сервером и отправляется обратно в том же виде (как эхо).

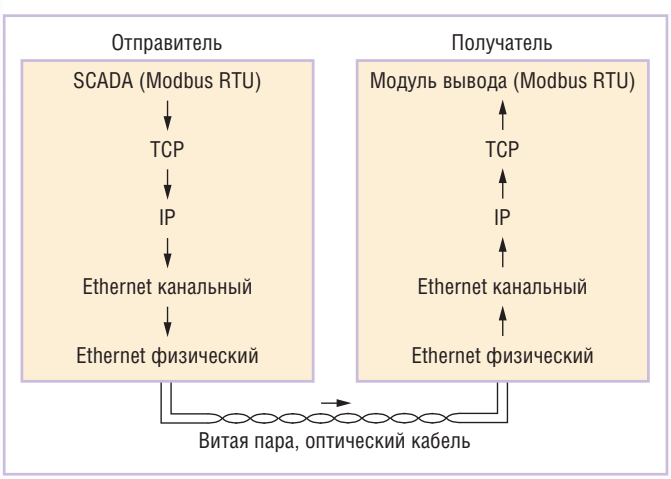

Рис. 4. Процесс передачи кадра Modbus RTU по уровням модели OSI через стек протоколов Ethernet TCP/IP в сетях с протоколом Modbus TCP

Изображённый на рис. 3 фрейм называется фреймом ADU, встраивается в поле «Данные» фрейма Ethernet [1] и посылается через TCP-порт 502, специально зарезервированный для Modbus TCP (порты назначаются и контролируются организацией IANA – Internet Assigned Numbers Authority, www.iana.org). Клиенты и серверы Modbus посылают, получают и прослушивают сообщения через TCP-порт 502.

Таким образом, структура кадра и смысл его полей «Код функции» и «Данные» для Modbus и Modbus TCP совершенно идентичны, поэтому для работы с Modbus TCP не требуется дополнительного обучения при знании Modbus RTU. Те же самые коды функций и данные, что и в Modbus RTU, передаются по очереди с прикладного (7-го) уровня модели OSI (рис. 4) на транспортный уровень, который добавляет к блоку PDU кадра Modbus RTU (рис. 1) заголовок с протоколом TCP. Далее новый полученный кадр передаётся на сетевой уровень, где в него добавляется заголовок IP, затем он передаётся на канальный уровень Ethernet и на физический. Дойдя до физического уровня, блок PDU оказывается «обросшим» заголовками протоколов всех уровней, через которые он прошёл. Пройдя по линии связи, сообщение продвигается снизу вверх по стеку протоколов (уровням модели OSI) в устройстве получателя, где на каждом уровне из него удаляется соответствующий заголовок, а на прикладном уровне выделяется блок PDU (код функции и данные) кадра протокола Modbus RTU.

В сети с протоколом Modbus TCP устройства взаимодействуют по типу «клиент–сервер», где в качестве клиента выступает ведущее устройство, в качестве сервера – ведомое. Сервер не может инициировать связи в сети, но некоторые устройства в сети могут выполнять роль как клиента, так и сервера.

Modbus TCP не имеет широковещательного или многоабонентского режима, он осуществляет соединение только между двумя устройствами. ●

Литература

1. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием. – М. : Горячая линия – Телеком, 2008. – 608 с.
2. Modbus over serial line specification and implementation guide, v1.02 [Электронный ресурс]. – Режим доступа : http://www.modbus.org. – Dec. 20, 2006. – 44 p.
3. Modbus application protocol specification v1.1a [Электронный ресурс]. – Режим доступа : http://www.modbus-IDA.org. – June 4, 2004. – 51 p.
4. Modicon Modbus Protocol Reference Guide. PI-MBUS-300 Rev. J. – MODICON, Inc., Industrial Automation Systems. – June 1996. – 121 p.
5. Modbus messaging on TCP/IP implementation guide, v1.0a [Электронный ресурс]. – Режим доступа : http://www.modbus-IDA.org. – June 4, 2004 – 46 p.