Джордж Томас

Введение в протокол Modbus

Часть 2. Modbus Serial и Modbus TCP

В статье продолжено рассмотрение протокола Modbus: описано его использование для передачи данных по последовательной линии связи, а также в сетях с протоколом TCP/IP.

Настоящий материал представляет собой вторую из двух статей, посвящённых протоколу Modbus. В ней рассматриваются две реализации этого протокола, основы построения которого были описаны в предыдущей статье (опубликована в «СТА» 2/2009. – Ред.). Первая реализация представляет собой традиционный вариант применения Modbus при передаче данных по последовательной линии связи. Вторая является более современной – в этом варианте протокол Modbus работает в сетях с протоколом TCP/IP. Обе реализации продолжают оставаться популярными.

Modbus в системах последовательной передачи данных

На сайте Modbus.org опубликовано руководство Modbus over Serial Line Specification and Implementation Guide V1.02, в котором содержатся указания по использованию Modbus с последовательными линиями передачи данных. Как упоминалось в предыдущей статье, протокол Modbus изначально был ориентирован на применение с соединениями «точка-точка» по интерфейсу EIA-232C (RS-232C). При этом в качестве ведущего устройства (master) в системе рассматривалось устройство человеко-машинного интерфейса (ЧМИ), а в качестве ведомого устройства (slave) – ПЛК. Наличие в системе множества ведомых и одного ведущего устройства предполагает наличие множества связей, что неудобно и дорого. Поэтому весьма естественным является переход от соединений «точка-точка» к многоточечной последовательной инфраструктуре, такой как EIA-485 (RS-485), которая позволяет одному ведущему устройству обмениваться информацией с множеством ведомых устройств по общей последовательной линии. Этот подход и освещается в упомянутом документе, размещённом на Modbus.org, но в исходном руководстве Modicon Modbus Reference Guide он не упомянут.

Трёхуровневая модель

В отличие от традиционной 7-уровневой сетевой модели OSI, принятой ISO, модель Modbus для передачи данных по последовательной линии связи (Modbus over Serial Line) «сжата» до трёх уровней, как это показано в таблице 1. Верхним является прикладной уровень, который был рассмотрен в предыдущей статье. Он именуется прикладным протоколом Modbus, или просто протоколом Modbus. Уровни 3–6 не используются – вместо них в данной модели выступает прикладной уровень, на котором обеспечивается сквозная передача сообщений. Канальный уровень (уровень 2) представлен Modbus-протоколом передачи данных по последовательной линии связи. Наконец, физический уровень (уровень 1) представлен интерфейсом RS-232C (EIA-232C) либо RS-485 (EIA-485). Трёхуровневый протокол Modbus для передачи данных по последовательной линии связи гораздо проще в понимании по сравнению с другими промышленными протоколами передачи данных. Поскольку прикладной протокол Modbus был подробно рас-

Таблица 1

Трёхуровневая модель Modbus для передачи данных по последовательной линии связи (Modbus over Serial Line)

Уровень	Функция в модели OSI	Функция в модели Modbus
7	Прикладной уровень	Прикладной протокол Modbus
3–6	Разные функции	Нет
2	Канальный уровень	Modbus-протокол для последовательной линии связи
1	Физический уровень	RS-232C, RS-485 (EIA-232C, EIA-485)

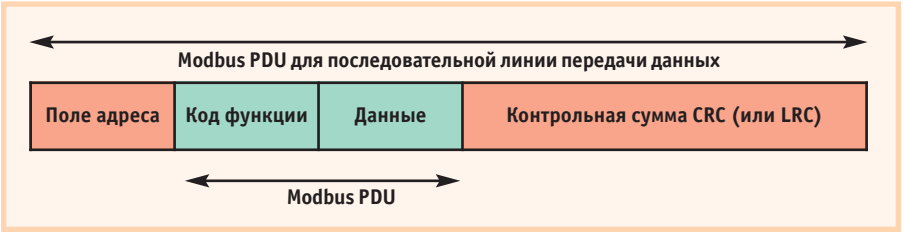

Рис. 1. Перед Modbus PDU находится поле адреса ведомого устройства, а после него – поле контрольной суммы

смотрен в предыдущей статье, здесь он не обсуждается. В данной статье описаны канальный и физический уровни.

Канальный уровень

В предыдущей статье были приведены сведения о структуре кадра сообщения, который включает в себя PDU – элементарный пакет протокола Modbus для последовательной линии передачи данных, тем не менее, дадим краткое описание. На рис. 1 показано, что PDU состоит из четырёх элементов.

В центре находится собственно Modbus PDU, содержащий два элемента – код функции и данные. В большинстве реализаций Modbus используется ограниченный набор кодов функций. При этом структура данных может варьироваться в зависимости от кода функции. В случае последовательной линии передачи данных перед Modbus PDU находится поле адреса, а после него – поле контрольной суммы. В поле адреса содержится только адрес ведомого устройства или адрес широковещательной передачи. Адрес ведущего устройства не требуется и не указывается, поскольку речь идет о протоколе «ведущий – ведомый», в котором команды исходят от уникального ведущего устройства.

Как говорилось в предыдущей статье, структура Modbus-сообщения для последовательной линии передачи данных зависит от того, какой режим используется – ASCII или RTU. На рис. 2 показана структура кадра для более распространённого режима RTU. Структура отличается компактностью – всего один байт занимает адрес ведомого устройства или адрес широковещательной передачи, один байт – код функции и два – контрольная сумма (CRC). Следует отметить, что в сообщении отсутствует последовательность, обозначающая конец кадра. В режиме RTU конец кадра отмечается паузой, равной времени передачи 3,5–4,5 символов.

Максимальное по длине сообщение занимает всего 256 байтов. В режиме RTU для передачи каждого байта необходимо 11 битов. Сам символ – это восемь битов, плюс стартовый и стоповый биты и один бит чётности. Если бит чётности не используется, то вместо него посылается ещё один стоповый бит. При использовании бита чётности осуществляется контроль на чётность либо на нечётность.

Формат сообщения в режиме ASCII, показанный на рис. 3, предусматривает

Адрес ведомого устройства	Код функции	Данные	Контрольная сумма (CRC)
1 байт	1 байт	От 0 до 252 байтов	2 байта (Младший байт | Старший байт)

Рис. 2. Структура кадра для режима RTU более компактная, чем для ASCII

Начало	Адрес ведомого устройства	Код функции	Данные	Контрольная сумма (LRC)	Конец
1 символ	2 символа	2 символа	От 0 до 2×252 символа	2 символа	2 символа (CR, LF)

Рис. 3. Структура кадра для режима ASCII предусматривает передачу символов начала и конца сообщения

два байта для адреса ведомого устройства и два байта для кода функции. В отличие от RTU в режиме ASCII используется 2-байтовая контрольная сумма LRC. Преимуществом формата ASCII является то, что сообщения в этом формате могут быть прочитаны человеком. Следует отметить, что в данном случае имеется последовательность, обозначающая конец сообщения и представленная управляющими символами CR (возврат каретки) и LF (перевод строки). При этом паузы в процессе передачи сообщения не имеют значения. Данные представляются в шестнадцатеричном формате в коде ASCII. Каждый символ ASCII требует всего 7 битов, но каждый байт данных представляется двумя символами. При этом используются один стартовый и один стоповый бит. Если используется бит чётности, то осуществляется контроль на чётность либо на нечётность. Если бит чётности не используется, то вместо него посылается ещё один стоповый бит. Это означает, что передача каждого байта в режиме ASCII выливается в передачу 10 битов.

Физический уровень

Изначально протокол Modbus разрабатывался с ориентацией на соединение «точка–точка» между главным компьютером и ПЛК через интерфейс RS-232C (EIA-232C). Этот вариант актуален и сегодня. Но спецификация протокола Modbus для передачи данных по последовательной линии обеспечивает возможность многоточечного соединения по стандарту RS-485 (EIA-485) – схему, поддерживающую до 32 устройств, подключённых к общей шине. Такая конфигурация может быть реализована с применением либо двухпроводного, либо четырёхпроводного подключения. В любом из вариантов последовательной передачи данных возможен широкий диапазон скоростей – от 1,2 до 115 кбит/с, но все реализации должны, как минимум, обеспечивать работу на скоростях 9,6 и 19,2 кбит/с. По умолчанию принимается значение скорости передачи данных 19,2 кбит/с.

Двухпроводная сеть

На рис. 4 показана рекомендуемая схема двухпроводной сети с интерфейсом RS-485 (EIA-485) с линейной поляризацией. В такой сети, естественно, имеется один узел, являющийся ведущим устройством, и множество ведомых узлов, подключённых к общей двухпроводной шине, провода которой обозначены как D0 и D1.

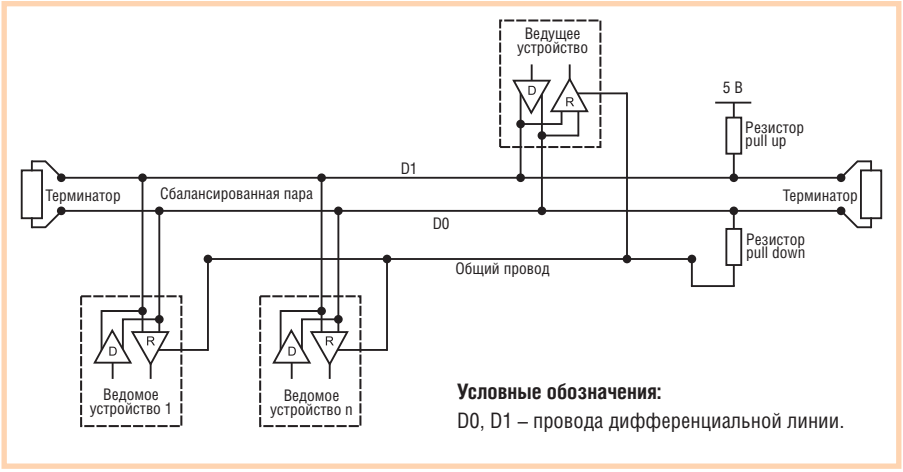

Рис. 4. Двухпроводная схема подключения фактически требует трёх проводов

Как минимум, такая схема обеспечивает поддержку 32 устройств. При использовании двухпроводной шины выход трансмиттера напрямую соединён со входом приёмника каждого из устройств. Несмотря на то что шина именуется двухпроводной, здесь имеется третий – общий (common) провод опорного потенциала, обозначенный на рисунке как «общий». Чтобы максимальное синфазное напряжение устройство не превышало установленного максимально допустимого значения, каждое устройство должно делить общий провод со всеми остальными устройствами, выходящими на шину. Резисторы pull up и pull down (подтягивающие резисторы) создают предопределённый уровень на линии передачи данных, когда ни один из узлов сети не передаёт данные. Для того чтобы приёмник RS-485 (EIA-485) мог фиксировать, что линия находится в состоянии off (отключено), требуется отказоустойчивое смещение 200 мВ. Такое подключение создаёт дополнительную помехоустойчивость системы. На обоих концах шины находятся терминаторы (LT), необходимые для согласования с волновым сопротивлением шины. Спецификация протокола Modbus для передачи данных по последовательной линии связи рекомендует, чтобы подтягивающие резисторы имели значения сопротивления в диапазоне от 450 до 650 Ом и чтобы использовалась только одна такая сеть. Следует отметить, что отказоустойчивое смещение вообще необходимо. Некоторые трансиверы имеют встроенные схемы смещения, и тогда потребность во внешнем смещении отпадает.

Четырёхпроводная сеть

На рис. 5 показана рекомендуемая схема четырёхпроводной сети с интерфейсом, где также применяются устройства RS-485 (EIA-485). В каждом из устройств передатчик и приёмник разделены. При этом передатчик ведущего устройства соединен с приёмниками всех ведомых устройств, а передатчики всех ведомых устройств соединены с приёмником ведущего устройства. Здесь также используются отказоустойчивое смещение и терминатор, но в четырёхпроводной сети они дублируются. В четырёхпроводной схеме требуется «пятый» провод, играющий роль общего.

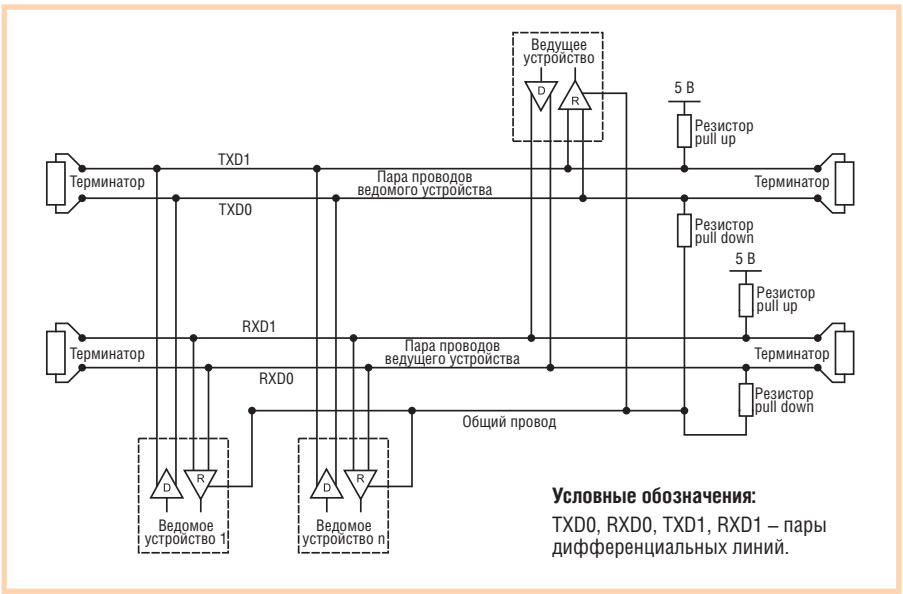

Рис. 5. Четырёхпроводная схема подключения фактически требует пяти проводов

Несмотря на то что спецификация протокола Modbus для передачи данных по последовательной линии связи поддерживает и двухпроводную, и четырёхпроводную схему, более популярной является первая. Хотя четырёхпроводная схема даёт возможность иметь полнодуплексную связь, сам протокол Modbus является строго полудуплексным. Ведущее устройство выдаёт команды конкретному ведомому устройству, в то время как ждёт ответа. Такой порядок вполне эффективно работает в двухпроводной схеме.

Modbus TCP

Протокол Modbus продолжает существовать в мире автоматизации, где сейчас больший интерес вызывает подключение к сетям Ethernet, а если говорить конкретнее, к сетям IP/Ethernet. С ориентацией на эту область применений на сайте Modbus.org опубликовано руководство Modbus Messaging on TCP/IP Implementation Guide V1.0b. Вместо трёхуровневой модели, которая существует в Modbus для передачи данных по последовательной линии связи, в Modbus TCP используется принятая для Интернет пятиуровневая модель, представленная в табл. 2.

Вместо пространного обсуждения вопросов физического и канального уровня в стандарте даётся ссылка на 1500-страничный стандарт IEEE 802.3. При этом не рассматривается, как физически подключать станции, какие провода или разъёмы применять. В данном сетевом стандарте говорится только о том, как Modbus PDU (содержащий код функции и данные) встроен в протокол более высокого уровня.

Ещё одним значительным отличием (рис. 6) является то, что в данном случае шина Modbus фактически является шиной IP. При этом физический и канальный уровни не конкретизируются. Вместо привычного ведущего устройства, к которому подключено множество ведомых устройств, используются термины «клиент» и «сервер». В качестве клиентов могут выступать устройства ЧМИ или ПЛК, а в качестве серверов – стойки сетевого оборудования. Аналогично ве-

Таблица 2

Пятиуровневая модель для Интернет в Modbus TCP

Уровень	Функция в модели OSI	Функция в модели Modbus
5, 6, 7	Прикладной уровень	Прикладной протокол Modbus
4	Транспортный уровень	Протокол управления передачей
3	Сетевой уровень	Интернет-протокол
2	Канальный уровень	IEEE 802.3
1	Физический уровень	IEEE 802.3

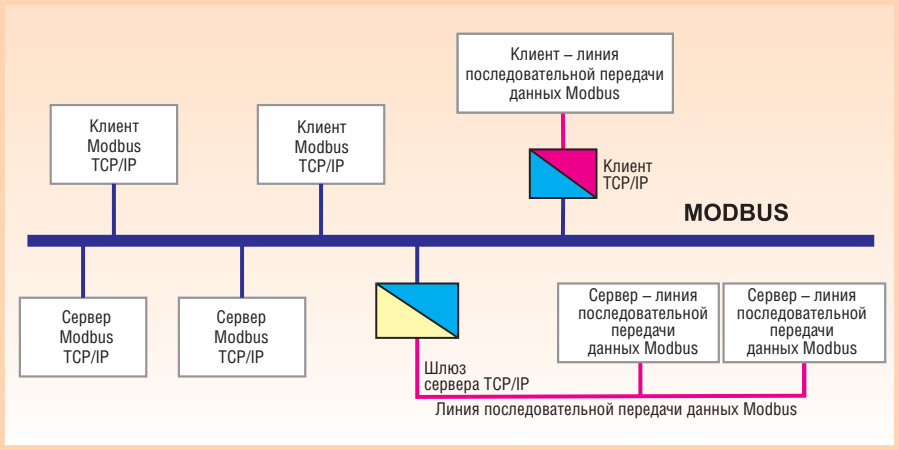

Рис. 6. В модели Modbus TCP используются клиенты и серверы вместо ведущих и ведомых

дущему устройству клиенты выдают команды серверу. Аналогично ведомому устройству серверы отвечают на команды клиента. Однако в точной терминологии взаимодействия между клиентом и сервером подразумевается, что клиенты выдают запросы, а серверы отвечают на них. В действительности процесс несколько сложнее:

- клиент с целью инициировать транзакцию посылает запрос (request);
- сервер посылает уведомление (indication), чтобы подтвердить, что запрос получен;
- сервер посылает ответ (response) во исполнение запроса клиента;
- клиент посылает подтверждение (confirmation) о получении ответа.

Важно подчеркнуть, что согласно этой модели в IP-сети может быть несколько клиентов, которые имеют доступ к общей группе серверов. В этом заключается фундаментальное отличие в работе данного варианта протокола Modbus. Здесь нет одного-единственного ведущего устройства, управляющего определённым набором ведомых устройств. Любое число клиентов может обращаться к любому числу серверов. Возможны ли конфликты, когда клиенты посылают несовместимые запросы к одному и тому же серверу? Да, возможны, но риск – это та цена, которую приходится платить за гибкость, предлагаемую данной моделью.

Заголовок MBAP

На рис. 7 показано, как формируется ADU (Application Data Unit) – прикладной пакет протокола Modbus TCP/IP.

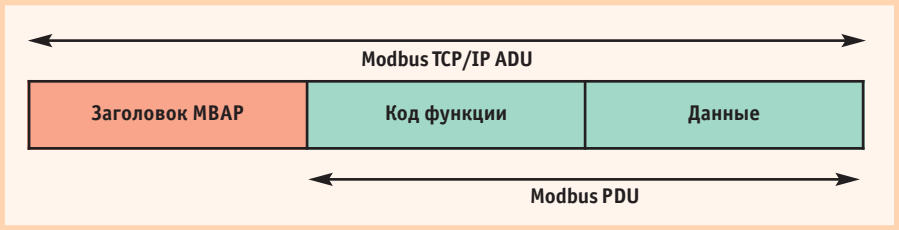

Рис. 7. К PDU Modbus добавляется заголовок MBAP

Традиционный Modbus PDU в приложении к последовательной линии передачи данных сохраняется – поля кода функции и данных присутствуют. В дополнение к PDU появляется заголовок MBAP, структура которого показана на рис. 8.

Идентификатор транзакции поступает от клиента и используется для отслеживания индивидуальных запросов. Сервер при ответе должен возвратить клиенту тот же самый идентификатор. Это позволяет клиенту посылать серверу множество запросов и не дожидаться получения ответа на каждый отдельный запрос. Наличие идентификатора протокола позволяет системе поддерживать несколько протоколов. Для Modbus этот идентификатор имеет значение 0. Поле длины содержит значение, равное длине всех остальных полей, включая поля PDU. И, наконец, поле идентификатора устройства содержит адрес ведомого устройства Modbus, доступ к которому должен осуществляться через шлюз.

Идентификатор транзакции	Идентификатор протокола	Длина	Идентификатор устройства
2 байта	2 байта	2 байта	1 байт

Рис. 8. Заголовок MBAP имеет длину 7 байтов

При взаимодействии клиентов и серверов Modbus TCP адресация станций реализуется с применением IP-адресов. Но если ведомое устройство Modbus подключено к последовательной линии передачи данных, то необходимо указать его фактический адрес. В этом случае в качестве IP-адреса будет выступать адрес шлюза. Для того чтобы переслать ADU по протоколу TCP, необходимо пользоваться зарегистрированным номером порта TCP. Сайт Modbus.org зарегистрировал для этой цели порт 502.

Заключение

Популярность протокола Modbus объясняется его простотой. А благодаря тому что знаниями Modbus обладает множество практикующих специалистов и этот открытый стандарт поддерживается ассоциацией Modbus-IDA, он продолжает оставаться популярным. ●

Автор — президент компании Contemporary Controls