

*Узбеков Ислон
магистр, кафедра вычислительной техники,
Национальный исследовательский университет Московский институт
электронной техники,
Россия, г. Москва
e-mail: uzbekov32@mail.ru*

ПРОТОКОЛ MODBUS

***Аннотация:** Рассматривается протокол Modbus и его применение в промышленности. Актуальность и причины популярности в автоматических системах. В работе также рассматриваются достоинства протокола по сравнению с другими, рассказывается о принципе работы и взаимосвязи с различными устройствами.*

Ключевые слова: протокол Modbus, Modbus master, Modbus slaves, Modbus RTU, Modbus ASCII/

*Uzbekov Islom
master student, department of computer engineering,
National Research University of Electronic Technology,
Russia, Moscow*

MODBUS PROTOCOL

***Abstract:** The Modbus Protocol and its application in the industry are considered. The relevance and the reasons for the popularity in automatic systems. The paper also discusses the advantages of the protocol in comparison with others, describes the principle of operation and the relationship with different devices.*

Keywords: Modbus Protocol, Modbus Master, Modbus Slaves, Modbus RTU, Modbus ASCII.

Modbus - это протокол, разработанный для обеспечения связи между подключенными к сети последовательными устройствами или приложениями. Протокол был введен корпорацией Modicon в 1979 году, прежде всего, для обеспечения связи в их программируемых логических контроллерах.

Modbus стал широко используемым протоколом, отчасти потому, что это открытый протокол, который производители могут использовать без затрат на лицензирование. Фактически - это стандартный протокол связи, используемый в производственной и промышленной сферах. Парадигма Master / Slave формирует

основу протокола Modbus. Связь осуществляется ведущим устройством, которое отправляет запросы ведомым устройствам, которые затем возвращают соответствующий ответ ведущему.

Сети Modbus обычно конфигурируются с одним ведущим устройством, которое может связываться и получать ответы от 1 до 247 ведомых устройств. Протокол Modbus широко используется в реализациях промышленной автоматизации, обеспечивая связь между многими датчиками и контроллерами, составляющими такие системы. Крупные предприятия часто используют несколько сетей Modbus для решения отдельных производственных процессов или производственных линий [1].

Режимы протокола

Modbus - это очень простой набор пакетных протоколов. Когда пакет декодируется независимо от «режима» передачи протокола, он содержит абсолютно одинаковое содержимое сообщения. Программные декодеры могут быть написаны с различными интерфейсами декодера / кодера для разных режимов передачи, а остальная часть программного обеспечения может быть унифицирована.

Когда Modbus передается по последовательным сетям типа RS232, RS422 и RS485, существует два стандартных режима передачи: ASCII или RTU (двоичный). Последовательная сеть должна иметь обозначение ASCII или RTU. Вы не можете смешивать режимы в одной сети. Процесс согласования отсутствует, возможности автоматической передачи тоже отсутствуют. Тип должен быть установлен разработчиком сети / системы один раз, и все устройства в сети должны быть вручную установлены на правильную скорость.

Modbus ASCII - это читаемый человеком формат передачи ASCII, который легко отлаживать на терминальном устройстве анализатора (устройстве, которое только прослушивает, но не управляет кабелем RS232 или RS485), поскольку терминальная программа будет отображать пакеты. Это анализировать в программном обеспечении очень легко, с уникальными

символами начала («:») и конечного пакета (CR-LF), но поскольку каждый байт отправляется в виде значения hex-ascii (например, «a» отправляется в виде двух байтов «2» и «1», представляющих шестнадцатеричный 0x21, который представляет собой «a»), это составляет половину скорости двоичный протокол передачи [2].

Каждый инициированный мастером пакет выглядит так:

Формат пакета Modbus ASCII (мастер-пакет)		
Название	Байты	Описание
Начало	1	«:» (ASCII 0x3A) символ начала пакета
Ведомый ID	2	ASCII идентификатора ведомого (например, идентификатор ведомого 0x2F отправляется в виде двух символов «2» и «F»)
Код функции	2	ASCII команды (называемый «кодом функции» или «FCxx», где xx - код)
Данные	меняется	Специфичные для команды данные в виде последовательности символов ASCII (2 на байт) в формате MSB
Контрольная сумма	2	Простая 8-битная контрольная сумма
Конец	2	Пакет завершения последовательности CR-LF

Каждый ведомый отвечает измененной версией пакета:

Формат пакета Modbus ASCII (подчиненный ответ)		
Название	Байты	Описание
Начало	1	«:» (ASCII 0x3A) символ начала пакета
Ведомый ID	2	ASCII ведомого идентификатора
Код функции	3	ASCII команды с установленным старшим битом в случае ошибки
Данные	меняется	Данные конкретных ответов команды
Контрольная сумма	2	Простая 8-битная контрольная сумма
Конец	2	Пакет завершения последовательности CR-LF

Режим Modbus ASCII имеет несколько преимуществ:

- легко отлаживать на терминальном устройстве анализатора (устройство, которое только прослушивает, но не управляет кабелем RS232 или RS485), поскольку терминальная программа может отображать пакеты в удобочитаемом формате, по 1 пакету на строку

- легко анализировать и сохранять синхронизацию в программном обеспечении, с уникальным начальным символом («:») и конечной последовательностью (CR-LF)

- меньшее / более простое программное обеспечение для вычисления 8-битной контрольной суммы, чем 16-битный CRC, используемый в режиме RTU, и несколько недостатков:

- половина скорости RTU: каждый байт передается как шестнадцатеричное значение ASCII, это половина скорости двоичного протокола передачи.

- менее надежный, чем RTU: 8-битная контрольная сумма гораздо более восприимчива к отсутствующим ошибкам, чем 16-битный CRC RTU.

Modbus RTU - это двоичный формат передачи. Каждый инициированный мастером пакет выглядит так:

Формат пакета Modbus RTU (мастер-пакет)		
Название	Байты	Описание
Ведомый ID	1	Идентификатор байта подчиненного целевого устройства
Код функции	1	Команда (называемая «кодом функции» или «FCxx»), где xx - код)
Данные	меняется	Отдельные данные команды в виде последовательности байтов в формате MSB, где это необходимо
CRC	2	16-битный CRC

Каждый ведомый отвечает измененной версией пакета:

Формат пакета Modbus ASCII (подчиненный ответ)
--

Название	Байты	Описание
Ведомый ID	1	Идентификатор байта подчиненного целевого устройства
Код функции	1	Тот же FC, что и мастер, запрошенный; старший бит установлен, если ошибка
Данные	меняется	Отдельные данные ответа команды в виде последовательности байтов в формате MSB, где это необходимо
CRC	2	16-битный CRC

Режим Modbus RTU имеет преимущества:

- быстрее, чем Modbus ASCII: один байт на символ, а не два
- более устойчивы к шуму, чем ASCII: 16-битный CRC лучше обнаруживает битовые ошибки, чем 8-битная контрольная сумма ASCII и несколько недостатков:

- сложнее написать программное обеспечение для синхронизации в шумной среде: нет последовательности начала / конца

- CRC требует больше программного обеспечения на ведомом устройстве для генерации / тестирования

- труднее отлаживать на терминальном устройстве sniffера: обычно требуется программа декодирования пакетов.

Список литературы:

1. Ревич Ю.В. Практическое программирование микроконтроллеров Atmel AVR на языке ассемблера. СПб.: БХВ-Петербург, 2008. 384 с.

2. Сахнюк А.А., Литвин А.М. Промышленные сети // Передовые технологии и технические решения. 2004. №2. С. 6-8.