

12+

Ленар Ильдарович

Садыков

Промышленные-сети Modbus-Ethernet диагностика

Ленар Садыков

**Промышленные сети.
Modbus-Ethernet диагностика**

«Издательские решения»

Садыков Л. И.

Промышленные сети. Modbus-Ethernet диагностика /
Л. И. Садыков — «Издательские решения»,

Практическое руководство для инженеров КИПиА и АСУТП, наладчиков и студентов профильных специальностей. Книга последовательно разбирает устройство и диагностику ключевых промышленных сетевых технологий: протокол Modbus (RTU, ASCII, TCP) со структурой кадров и кодами функций, физику и коммутацию Industrial Ethernet с резервированием колец, смежные полевые шины PROFIBUS DP, HART и CAN/CANopen, а также интеграцию с верхним уровнем через OPC UA и MQTT.

© Садыков Л. И.

© Издательские решения

Содержание

1.3. Топологии промышленных сетей	7
1.4. Среды передачи данных	8
2.9. Встроенные ограничения протокола	14
Конец ознакомительного фрагмента.	15

Промышленные сети. Modbus-Ethernet диагностика

Ленар Ильдарович Садыков

© Ленар Ильдарович Садыков, 2026

ISBN 978-5-0071-4445-2

Создано в интеллектуальной издательской системе Ridero

Глава 1. Введение в промышленные сети и модель OSI для АСУТП

1.1. Зачем нужны промышленные сети

Любая современная автоматизированная система управления технологическим процессом (АСУТП) представляет собой не набор изолированных приборов, а распределённую систему, в которой датчики, исполнительные механизмы, контроллеры, станции операторов и серверы верхнего уровня непрерывно обмениваются данными. Чем крупнее и сложнее объект автоматизации, тем больше в нём точек измерения и управления, и тем менее реалистично соединять каждое устройство с каждым отдельным проводом по схеме «точка-точка». Промышленная сеть решает эту задачу: она позволяет объединить десятки и тысячи устройств в единую инфраструктуру передачи данных, используя относительно небольшое число физических линий связи.

Помимо экономии на кабельной продукции и монтажных работах, промышленные сети дают возможность передавать не только базовое значение измеряемой величины, но и диагностическую информацию о состоянии прибора, вести удалённую настройку и калибровку, синхронизировать работу множества устройств во времени и интегрировать данные технологического процесса с системами более высокого уровня — от SCADA до ERP предприятия.

Важно. Промышленные сети принципиально отличаются от офисных (корпоративных) компьютерных сетей требованиями к детерминированности, реальному времени, устойчивости к электромагнитным помехам и допустимому времени восстановления после отказа. Перенос офисных практик построения сети на технологический уровень без учёта этой специфики — частая причина проблем на объектах автоматизации.

1.2. Эталонная модель OSI и её применение в промышленных сетях

Для описания и сравнения различных сетевых технологий традиционно используется семиуровневая эталонная модель взаимодействия открытых систем (OSI). В промышленных сетях, как правило, реально задействованы не все семь уровней в чистом виде — многие протоколы полевого уровня объединяют функции нескольких уровней модели в одном стеке, — однако сама модель остаётся удобным инструментом для понимания того, на каком этапе передачи данных может возникнуть та или иная неисправность.



Классический пример «сжатой» модели — Modbus RTU поверх интерфейса RS-485: здесь реализованы только физический и канальный уровни в узком смысле плюс прикладной протокол Modbus непосредственно поверх них, без полноценных сетевого и транспортного уровней. В противоположность этому Modbus TCP использует полный стек TCP/IP, добавляя сетевой и транспортный уровни поверх Ethernet, что даёт маршрутизацию, но одновременно вносит дополнительные источники задержек и точек отказа (коммутаторы, маршрутизаторы, сетевые стеки операционных систем).

1.3. Топологии промышленных сетей

Топология определяет физическую и/или логическую схему соединения устройств в сети и напрямую влияет на надёжность, стоимость монтажа и удобство диагностики.

Шинная топология (bus)

Все устройства подключаются к общей линии связи (шине), на концах которой устанавливаются согласующие резисторы (терминаторы). Классический пример — RS-485 в Modbus RTU и Profibus DP. Преимущество — минимальный расход кабеля; недостаток — обрыв шины в любой точке нарушает связь со всеми устройствами, расположенными за местом обрыва относительно ведущего узла.

Топология «звезда» (star)

Каждое устройство подключается отдельным кабелем к центральному коммутатору или концентратору. Типична для Industrial Ethernet. Обрыв одного луча звезды выводит из строя только одно устройство, не затрагивая остальные, однако отказ центрального коммутатора выводит из строя весь сегмент.

Кольцевая топология (ring)

Устройства соединяются последовательно, образуя замкнутое кольцо; при использовании протоколов резервирования кольца (например, RSTP, MRP, HSR) обрыв в одной точке кольца не приводит к потере связи, так как трафик автоматически перенаправляется в обратном направлении. Кольцевая топология с резервированием — стандартное решение для критичных сегментов промышленного Ethernet.

Древовидная и смешанная топологии

На практике крупные объекты автоматизации почти всегда используют комбинацию топологий: кольца или резервированные звёзды на магистральном уровне между шкафами и цехами, и простые шины или звёзды на уровне подключения конечных полевых устройств внутри одного шкафа или локальной зоны.

Совет. При проектировании и последующей диагностике сети полезно всегда иметь под рукой актуальную схему топологии — без неё локализация обрыва или определение границы сегмента, потерявшего связь, занимает значительно больше времени.

1.4. Среда передачи данных

Выбор физической среды передачи данных определяется требованиями по дальности, помехозащищённости, взрывобезопасности и стоимости.



1.5. Иерархическая модель автоматизации предприятия

Для понимания места конкретной промышленной сети в общей архитектуре предприятия удобно использовать общепринятую иерархическую модель (по мотивам стандарта ISA-95), выделяющую несколько уровней:

1. Уровень 0 — датчики и исполнительные механизмы (полевой уровень)
2. Уровень 1 — контроллеры и модули ввода/вывода, непосредственно управляющие процессом
3. Уровень 2 — станции операторов, SCADA/HMI, серверы сбора данных цеха или участка
4. Уровень 3 — системы управления производством (MES), диспетчеризация предприятия
5. Уровень 4 — корпоративные системы планирования ресурсов (ERP) и бизнес-аналитика

Каждому уровню исторически соответствуют свои протоколы и требования к сети: на уровне 0—1 доминируют детерминированные протоколы реального времени (Modbus, Profibus, CAN), на уровне 2—3 — Industrial Ethernet и протоколы интеграции (OPC UA), а на уровне 3—4 — стандартные ИТ-протоколы и облачные/MQTT-интеграции. Понимание того, к какому уровню относится диагностируемая проблема, часто сразу сужает круг вероятных причин: сбой на уровне 0—1 почти всегда связан с физической средой или детерминированной шиной, тогда как проблема на уровне 3—4 — это, как правило, вопрос ИТ-инфраструктуры и интеграции.

Важно. Смещение уровней — например, прямое подключение офисного ноутбука к технологической сети уровня 0—1 — является одной из самых частых причин как сетевых сбоев, так и инцидентов кибербезопасности на производстве. Этому вопросу отдельно посвящена глава 8.

1.6. Требования, специфичные для промышленных сетей

При проектировании, эксплуатации и диагностике промышленных сетей необходимо учитывать ряд требований, отличающих их от типовых офисных сетей:

- Детерминированность — гарантированное время доставки критичных данных, а не только средняя пропускная способность
- Работа в реальном времени — для контуров регулирования важна не просто доставка пакета, а доставка в пределах заданного цикла управления
- Высокая устойчивость к электромагнитным помехам от силового оборудования
- Расширенный температурный диапазон и устойчивость к вибрации для оборудования, устанавливаемого вне отапливаемых помещений
- Возможность длительной непрерывной работы (годы) без перезагрузки и без плановых окон обслуживания, характерных для офисных ИТ-систем
- Совместимость нового оборудования со значительно более старыми устройствами, которые могут эксплуатироваться десятилетиями

Эти требования объясняют, почему на промышленном объекте до сих пор массово встречаются, казалось бы, «устаревшие» технологии вроде RS-485 и Modbus RTU: их детерминированность, простота и предсказуемость поведения при отказах во многих случаях ценятся выше, чем более высокая пропускная способность современных решений.

В следующих главах книги мы последовательно разберём устройство и практическую диагностику наиболее распространённых промышленных сетевых технологий — начиная с протокола Modbus как наиболее массового и универсального, и заканчивая вопросами интеграции с верхним уровнем и кибербезопасности.

Глава 2. Протокол Modbus: RTU, ASCII, TCP — структура и функции

2.1. Место Modbus среди промышленных протоколов

Modbus был разработан компанией Modicon (ныне Schneider Electric) в 1979 году для собственных программируемых контроллеров и впоследствии стал открытым, свободно публикуемым протоколом. Простота структуры, отсутствие лицензионных отчислений и лёгкость программной реализации сделали Modbus фактическим стандартом де-факто для промышленной автоматизации: сегодня его поддерживает подавляющее большинство контроллеров, преобразователей частоты, счётчиков электроэнергии, измерительных приборов и модулей ввода/вывода независимо от производителя.

Исторически протокол существует в трёх основных вариантах передачи: Modbus RTU и Modbus ASCII — для последовательных интерфейсов (RS-485, RS-232), и Modbus TCP — для передачи поверх сетей Ethernet/IP. Все три варианта используют единую логическую модель данных и один и тот же набор кодов функций, различаясь лишь способом кодирования кадра и физической средой передачи.

2.2. Сравнение вариантов Modbus



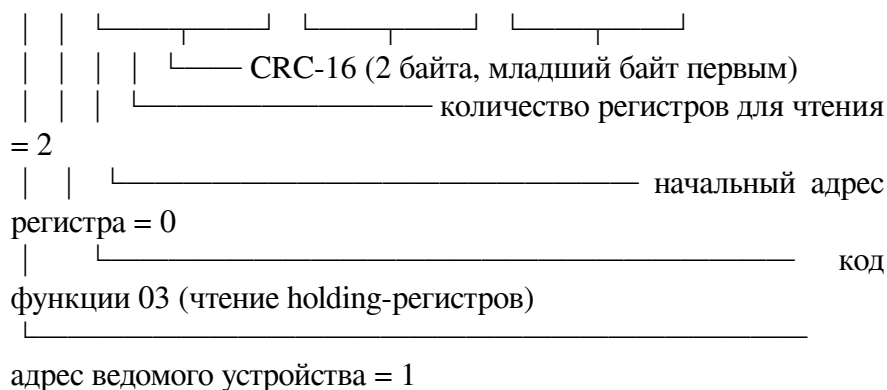
Важно. Modbus ASCII на практике встречается значительно реже RTU и TCP — в основном на устаревшем оборудовании или там, где требуется передача по каналам, не поддерживающим прозрачную передачу произвольных двоичных данных (например, некоторые модемные и радиоканалы). В большинстве современных проектов достаточно уверенно владеть Modbus RTU и Modbus TCP.

2.3. Структура кадра Modbus RTU

Кадр Modbus RTU состоит из четырёх основных полей, передаваемых без дополнительных стартовых/стоповых символов между ними — границы кадра определяются исключительно по паузам в эфире длительностью не менее 3,5 периода передачи символа:

1. Адрес устройства (1 байт) — адрес ведомого устройства от 1 до 247; адрес 0 зарезервирован для широковещательной передачи
2. Код функции (1 байт) — определяет операцию (чтение регистров, запись и т.д.)
3. Данные (переменная длина) — параметры функции и/или считываемые значения
4. Контрольная сумма CRC-16 (2 байта) — используется для обнаружения ошибок передачи

01 03 00 00 00 02 C4 0B



Приведённый пример — типичный запрос на чтение двух regs (holding registers), начиная с адреса 0, у устройства с адресом 1. При работе с анализатором шины или логическим анализатором понимание этой структуры позволяет буквально «читать» перехваченный трафик побайтово, не прибегая к специализированному ПО.

2.4. Особенности кадра Modbus ASCII

В отличие от RTU, кадр ASCII начинается с символа «:» (двоеточие) и завершается последовательностью CR LF (возврат каретки и перевод строки), а все байты данных передаются в виде пар ASCII-символов, кодирующих шестнадцатеричные цифры. Это делает кадр примерно вдвое длиннее по числу передаваемых символов по сравнению с RTU, зато позволяет визуально читать содержимое кадра без специального декодера и использовать 7-битные каналы связи.

2.5. Структура Modbus TCP и инкапсуляция

Modbus TCP переносит тот же прикладной уровень (код функции и данные) внутри TCP-соединения на стандартном порту 502, добавляя в начало каждого сообщения заголовок MVAR (Modbus Application Protocol header) длиной 7 байт:

1. Идентификатор транзакции (2 байта) — используется клиентом для сопоставления запросов и ответов при параллельных обращениях
2. Идентификатор протокола (2 байта) — всегда 0 для Modbus
3. Длина (2 байта) — количество последующих байт сообщения
4. Идентификатор модуля, Unit ID (1 байт) — используется преимущественно при обращении через шлюз Modbus TCP/RTU к конкретному устройству на последовательной шине за шлюзом

Контрольная сумма CRC в Modbus TCP не передаётся — целостность данных обеспечивается на транспортном уровне средствами TCP/IP. Это важно понимать при анализе трафика: в TCP-версии протокола отсутствие CRC в кадре — не ошибка, а нормальное поведение протокола.

Совет. Многие промышленные шлюзы Modbus TCP/RTU по умолчанию игнорируют или произвольно подставляют Unit ID. При диагностике сети со шлюзом всегда в первую очередь проверяйте соответствие настроенного в SCADA/контроллере Unit ID реальному адресу устройства на стороне последовательной шины — рассогласование этого параметра является одной из самых частых причин «необъяснимой» потери связи через шлюз.

2.6. Модель данных Modbus

Все данные в Modbus логически организованы в четыре независимых адресных пространства, различающихся по типу доступа (чтение/запись) и размерности:



Важно. На практике очень многие производители приборов не соблюдают строгое разделение между Input Registers и Holding Registers, публикуя измеренные значения через регистры хранения (Holding Registers, функция 03) вместо входных регистров (функция 04). При интеграции нового устройства всегда сверяйтесь с картой регистров конкретного прибора, а не полагайтесь на «типовое» распределение по спецификации.

2.7. Основные коды функций Modbus



При возникновении ошибки на стороне ведомого устройства (недопустимый адрес, недопустимое значение, внутренняя ошибка устройства) в ответе устанавливается старший бит кода функции (то есть, например, вместо 03 возвращается 83), а следом передаётся однобайтовый код исключения, поясняющий причину отказа — это первое, на что стоит смотреть при анализе перехваченного трафика с признаками сбоя обмена.

2.8. Модель master/slave (client/server) и адресация

Классический Modbus RTU/ASCII построен по модели «ведущий — ведомый» (master/slave): инициатором любого обмена всегда выступает единственное ведущее устройство на шине (как правило, контроллер или шлюз), а ведомые устройства только отвечают на запросы и никогда не передают данные по собственной инициативе. В терминологии Modbus TCP эту же модель принято называть «клиент — сервер».

Наличие только одного ведущего устройства на шине RTU — не рекомендация, а жёсткое ограничение протокола: одновременное подключение двух независимых мастеров к одной

шине RS-485 приводит к коллизиям и непредсказуемому поведению сети. Если по проекту необходим доступ к одним и тем же приборам одновременно и от SCADA, и от локальной панели оператора, для этого используются либо программные посредники (шлюзы, агрегирующие запросы от нескольких клиентов Modbus TCP и опрашивающие шину RTU от единственного физического мастера), либо разделение приборов по разным независимым шинам.

Отдельный частный случай адресации — широковещательная передача (broadcast) с адресом устройства 0 в Modbus RTU/ASCII: такой запрос выполняют все устройства на шине без отправки ответа. Broadcast поддерживается только для функций записи и требует, чтобы все устройства на шине корректно его обрабатывали, — на практике поддержка широковещательных команд у разных производителей может отличаться, поэтому её использование в ответственных проектах рекомендуется отдельно проверять на реальном оборудовании.

2.9. Встроенные ограничения протокола

При всей своей универсальности классический Modbus обладает рядом принципиальных ограничений, которые необходимо учитывать на этапе проектирования системы:

- Отсутствие встроенной аутентификации — любое устройство, физически подключённое к шине или имеющее сетевой доступ к порту 502, может отправлять команды записи без какой-либо проверки прав

- Отсутствие шифрования данных — весь трафик передаётся в открытом виде

- Ограничение адресного пространства RTU/ASCII 247 устройствами на одну физическую шину

- Отсутствие стандартизированного механизма отчёта об изменении значения (report-by-exception) в классической спецификации — опрос всегда инициируется мастером (хотя отдельные расширения и профили это частично компенсируют)

Важно. Отсутствие аутентификации и шифрования в протоколе Modbus — не недостаток конкретной реализации, а изначальная особенность спецификации, рассчитанной на изолированные технологические сети. Вопросы защиты сетей на основе Modbus от несанкционированного доступа подробно рассматриваются в главе 8, посвящённой кибербезопасности промышленных сетей.

В следующей главе мы перейдём от теоретической структуры протокола к практике: рассмотрим типичные настройки последовательного порта и сети для Modbus RTU/TCP, инструменты для отладки обмена и методику последовательной диагностики при потере связи с устройством или группой устройств.

Глава 3. Практика Modbus: настройка, отладка, диагностика неисправностей

3.1. Параметры последовательного порта для Modbus RTU

Для корректной связи по Modbus RTU у всех устройств на одной шине RS-485 должны совпадать четыре параметра последовательного порта: скорость передачи (baud rate), количество бит данных, чётность (parity) и количество стоповых бит. Наиболее распространённая комбинация — 9600 или 19200 бод, 8 бит данных, без контроля чётности (None), 1 стоповый бит (сокращённо обозначается как 8N1), однако конкретные значения всегда определяются проектом и должны быть одинаковы для всех узлов шины.

Важно. Несовпадение хотя бы одного из четырёх параметров порта — самая частая причина полного отсутствия связи с новым или недавно заменённым устройством. Прежде чем подозревать обрыв линии или неисправность прибора, всегда в первую очередь сверяйте все четыре параметра порта на устройстве и на мастере.

3.2. Расчёт времени ожидания ответа (timeout)

Тайм-аут ожидания ответа от ведомого устройства должен учитывать не только время физической передачи кадра на выбранной скорости, но и собственное время обработки запроса устройством (может достигать десятков и сотен миллисекунд для приборов с медленным микроконтроллером), а также накопленную задержку при опросе через промежуточные шлюзы. Слишком короткий тайм-аут приводит к ложным «потерям связи» с полностью исправными, но медленно отвечающими устройствами; слишком длинный — снижает общую скорость опроса всей шины при реальном отказе одного из устройств.

- Начинайте настройку с тайм-аута, рекомендованного производителем конкретного устройства, если он указан в документации

- При отсутствии рекомендации — ориентируйтесь на удвоенное время передачи максимального по длине кадра на выбранной скорости плюс запас 100—200 мс на обработку

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.