УДК 681.5

ЗАСТОСУВАННЯ КОМУНІКАЦІЙНОГО ПРОТОКОЛУ MODBUS ДЛЯ ОБМІНУ ДАНИМИ МІЖ ЕЛЕМЕНТАМИ СИСТЕМ АВТОМАТИЗАЦІЇ

Лісовець С. М., Коляда Д. М.

Київський національний університет технологій та дизайну

Розглянуто обмін даними між елементами систем автоматизації, такими як ОВЕН ПЛК150, та персональним комп'ютером з автоматичним перетворювачем інтерфейсів ОВЕН USB/RS-485 АС4 і маршрутизатором TP-LINK 740n, по протоколах Modbus RTU і Modbus TCP. Встановлено, що, окрім швидкості обміну даними, обидва протоколи забезпечують однакові функції для обміну даними і приблизно однакову надійність.

Ключові слова: *ведений пристрій, ведучий пристрій, кадр, комунікаційний протокол, лінія передачі, модулі введення/виведення, мережевий обмін, промислова мережа, широкомовний режим*

Комунікаційний протокол Modbus і однойменна мережа є найбільш розповсюдженими у світі серед протоколів і мереж. Незважаючи на свій вік (протокол Modbus став стандартом ще в 1979 р.) він не тільки не застарів, але, навпаки, демонструє суттєво зрослу кількість орієнтованих на нього нових розробок і об'єм організаційної підтримки, який постійно зростає. Мільйони Modbus-пристроїв по всьому світу продовжують успішно працювати, обновлюються версії опису протоколу Modbus [1].

В Україні протокол Modbus по розповсюдженості конкурує тільки з PROFIBUS. Популярність протоколу Modbus в теперішній час пояснюється, насамперед, сумісністю з великою кількістю обладнання, яке підтримує протокол Modbus. Крім того, протокол Modbus має високу вірогідність передачі даних, яка пов'язана із надійним методом контролю похибок. Протокол Modbus дозволяє уніфікувати команди обміну завдяки стандартизації номерів (адрес) регістрів і функцій їх зчитування/запису. Основним недоліком протоколу Modbus є мережевий обмін по типу «ведучий/ведений», що не дозволяє веденим пристроям передавати дані зразу після їх появи і тому потребує інтенсивного опитування ведених пристроїв ведучими пристроями. Різновидами протоколу Modbus виступають протокол Modbus Plus [1], який представляє собою багатомастерний протокол з кільцевою передачею маркера, і протокол Modbus TCP [1], який розрахований на застосування в мережах Ethernet.

© Київський національний університет технологій та дизайну, 2016

Протокол Modbus має два режими передачі: RTU (Remote Terminal Unit – віддалений термінальний пристрій) і ASCII. Стандарт передбачає, що режим RTU в протоколі Modbus повинен бути присутнім обов'язково, а режим ASCII є опціонним (необов'язковим). Користувач може вибирати будь-який з них, але всі модулі, які під'єднані до мережі Modbus, повинні мати один і той же режим передачі [2, 3].

В основному буде розглядатися протокол Modbus RTU, оскільки протокол Modbus ASCII в Україні практично не застосовується. Необхідно відмітити, що протокол Modbus ASCII не треба плутати з протоколом DCON, який застосовується в модулях фірм Advantech і ICP DAS та не відповідає стандарту Modbus.

Стандарт Modbus передбачає застосування фізичних інтерфейсів RS-485, RS-422 або RS-232. Для організації промислових мереж найбільш часто застосовується двохпровідний інтерфейс RS-485. Для з'єднань типу «точка-точка» може бути застосовані інтерфейси RS-422 або RS-232.

В стандарті Modbus є вимоги обов'язкові, рекомендуємі і опціонні (необов'язкові). Існує три ступеня відповідності стандарту: повністю відповідає (коли протокол відповідає всім обов'язковим вимогам і всім рекомендуємим вимогам), умовно відповідає (коли протокол відповідає тільки обов'язковим вимогам і не відповідає рекомендуємим вимогам) і не відповідає. Модель OSI протоколу Modbus утримує три рівня: фізичний, канальний і прикладний [4, 5].

В нових розробках на основі протоколу Modbus стандарт рекомендує застосовувати інтерфейс RS-485 з двохпровідною лінією передачі, але допускає застосування інтерфейсу RS-232 з чотирьохпровідною лінією передачі.

Шина Modbus повинна складатися з одного магістрального кабелю, від якого можуть бути зроблені відводи. Магістральний кабель Modbus повинен утримувати три провідника в загальному екрані, два з яких повинні представляти собою кручену пару, а третій повинен з'єднувати загальні («земляні») виводи всіх інтерфейсів RS-485 в мережі. Загальний провідник і екран повинні бути заземлені в одній точці, причому бажано біля ведучого пристрою. Пристрої можуть підключатися до кабелю трьома способами: безпосередньо до магістрального кабелю, через пасивний розгалужувач (трійник) і через активний розгалужувач, який утримує розв'язуючий повторювач інтерфейсу [6, 7].

Пристрої Modbus обов'язково повинні підтримувати швидкості обміну 9600 і 19200 біт/с, з них 19200 біт/с встановлюється за замовчуванням. Допускаються

© Київський національний університет технологій та дизайну, 2016

швидкості 1200, 2400, 4800, …, 38400 біт/с, а також 65, 115 кбіт/с. Швидкість передачі повинна витримуватися в передавачі з похибкою не гірше 1%, а приймач повинен приймати дані при відхиленні швидкості передачі до 2%.

Протокол Modbus передбачає, що тільки один ведучий пристрій (контролер) і до 247 ведених пристроїв (модулів введення/виведення) можуть бути об'єднані в промислову мережу. Обмін даними завжди ініціюється ведучим. Ведені пристрої ніколи не починають передачу даних, поки не отримають запит від ведучого. Також ведені пристрої не можуть обмінюватися даними один з одним. Тому в будь-який момент в мережі Modbus може здійснюватися тільки один акт обміну даними.

Адреси з 1 по 247 є адресами Modbus-пристроїв в мережі, а адреси з 248 по 255 зарезервовані. Ведучий пристрій не повинен мати адреси, і в мережі не повинно бути двох або більше пристроїв з однаковими адресами. Ведучий пристрій може посилати запити всім веденим пристроям одночасно (широкомовний режим) або тільки одному.

Для широкомовного режиму зарезервована адреса 0 (при використанні в команді цієї адреси вона приймається всіма пристроями мережі).

Постановка завдання

В протоколі Modbus RTU повідомлення починає сприйматися як нове після паузи (тиші) на шині тривалістю не менше 3,5 шістнадцяткових символів (14 біт), тобто значення паузи залежить від швидкості передачі. Формат кадру (фрейму) протоколу Modbus показний на рис. 1. Тут ADU (Application Data Unit) – елемент даних програми, PDU (Protocol Data Unit) – елемент даних протоколу.

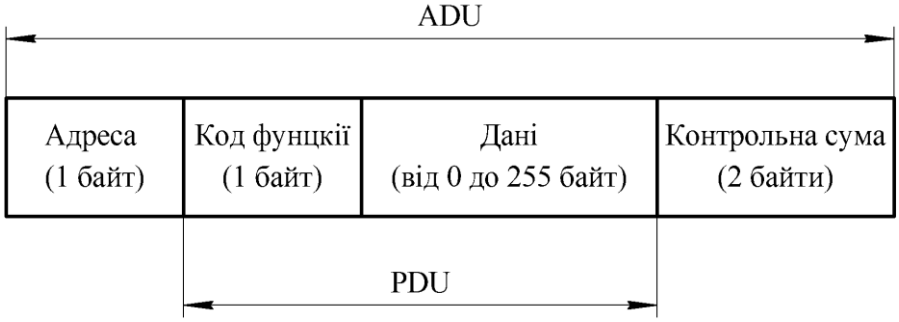

Рис. 1. **Формат кадру (фрейму) протоколу Modbus**

Поле «Адреса» завжди (навіть у відповідь на команду, яку надіслав ведучий) утримує тільки адресу веденого пристрою. Завдяки цьому ведучий пристрій знає, від

© Київський національний університет технологій та дизайну, 2016

якого веденого пристрою прийшла відповідь. Поле «Код функції» вказує веденому пристрою на те, яку дію необхідно виконати. Поле «Дані» може утримувати довільну кількість байт в діапазоні від 0 до 255. В ньому може утримуватися інформація про параметри, які використовуються в запитах контролера або у відповідях модуля. Поле «Контрольна сума» утримує контрольну суму (CRC16) довжиною 2 байти.

Протокол Modbus TCP (інша назва – Modbus TCP/IP) використовується для того, щоб підключити пристрої з протоколом Modbus до мережі Ethernet або до мережі Internet. Він використовує протоколи Ethernet на 1-му і 2-му рівнях моделі OSI, протоколи TCP і IP на 3-му і 4-му рівнях моделі OSI, а також кадри Modbus RTU на 7-му (прикладному) рівні моделі OSI. Тобто Ethernet TCP/IP використовується для транспортування модифікованих кадрів Modbus RTU.

Кадр Modbus RTU (див. рис. 1) в цьому випадку не має контрольної суми, оскільки застосовується стандартна контрольна сума Ethernet TCP/IP. Також немає поля «Адреса», оскільки в Ethernet застосовується інша система адресації. Таким чином, тільки два поля – «Код функції» і «Дані» (блок PDU) вбудовуються в протокол Ethernet TCP/IP. Перед ними вставляється нове поле MBAP (ModBus Application Protocol – прикладний протокол Modbus) (див. рис. 2).

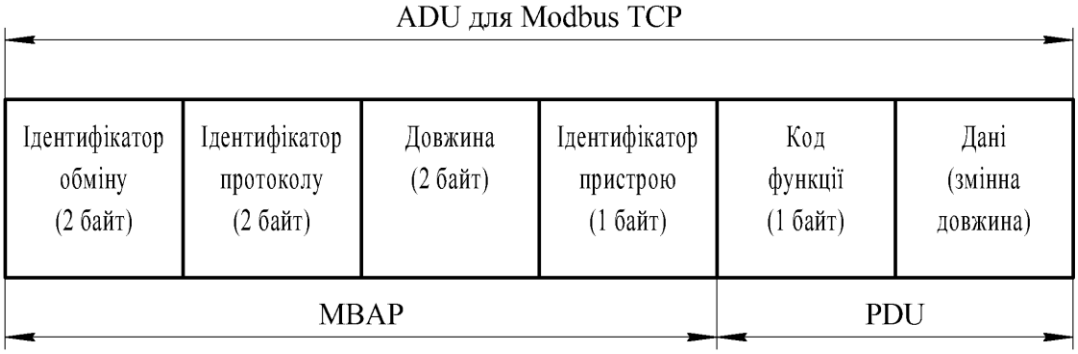

Рис. 2. **Частина кадра Modbus TCP, яка вбудовується в поле «Дані» кадру Ethernet**

Поле «Ідентифікатор обміну» використовується для ідентифікації повідомленням у випадку, коли в межах одного TCP-з'єднання клієнт посилає серверу кілька повідомлень без отримання відповіді після кожного повідомлення. Поле «Ідентифікатор протоколу» утримує лог. 0 і зарезервоване для майбутніх застосувань. Поле «Довжина» утримує кількість байт, які розташовуються за ним. Поле «Ідентифікатор пристрою» ідентифікує віддалений сервер, яка розташовується зовні мережі Ethernet (наприклад, в мережі Modbus RTU, яка з'єднана с мережею Ethernet за

© Київський національний університет технологій та дизайну, 2016

допомогою шлюзу). Найчастіше поле «Ідентифікатор пристрою» утримує лог. 0 або лог. 1, ігнорується сервером і відправляється назад в такому ж самому вигляді (як луна).

Кадр, який зображений на рис. 2, називається кадром ADU. Він вбудовується в поле «Дані» кадру Ethernet і посилається через TCP-порт 502, який спеціально зарезервований для протоколу Modbus TCP (необхідно зауважити, що порти призначаються і контролюються організацією IANA – Internet Assigned Numbers Authority). Клієнти і сервери Modbus посилають, отримують і прослуховують повідомлення через TCP-порт 502. Структура кадра і смисл його полів «Код функції» і «Дані» для Modbus і Modbus TCP абсолютно ідентичні, тому для роботи з Modbus TCP немає потреби в додатковому навчанні при умові знання того, як функціонує Modbus RTU.

В мережі з протоколом Modbus TCP пристрої взаємодіють по типу «клієнт-сервер», де в якості клієнта виступає ведучий пристрій, а в якості сервера – ведений пристрій. Сервер не може ініціювати зв'язок в мережі, але деякі пристрої в мережі можуть виконувати функцію як клієнта, так і сервера. Також необхідно зауважити, що протокол Modbus TCP не має широкомовного або багатоабонентського режимів роботи, він здійснює з'єднання тільки між двома пристроями.

Результати досліджень

Дослідження комунікаційного протоколу Modbus виконувалося за допомогою програмуємого логічного контролера ОВЕН ПЛ150 (з однієї сторони) і персонального комп'ютера з автоматичним перетворювачем інтерфейсів USB/RS-485 ОВЕН АС4 (для роботи по протоколу Modbus RTU) і маршрутизатором TP-LINK 740n (для роботи по протоколу Modbus TCP). В якості лінії зв'язку довжиною кілька десятків метрів застосовувалися відповідно кабель КСПП ТУ У 05758730.010 виробництва Одескабель і кручена пара категорії 5е.

Для читання стану дискретних входів контролера ОВЕН ПЛ150 застосовувалася функція 02, читання стану дискретних виходів – функція 01, читання двійкового умісту вхідних регістрів – функція 04, читання двійкового умісту вихідних регістрів – функція 03.

Дослідження показали високу надійність передачі даних як із застосуванням протоколу Modbus RTU, так і із застосуванням протоколу Modbus TCP. Так як обмін даними по протоколах Modbus RTU і Modbus TCP виконувався виключно із застосуванням стандартних функцій 01, 02, 03, 04 (та деяких інших), то з точки зору

© Київський національний університет технологій та дизайну, 2016

обміну даними різниці між Modbus RTU і Modbus TCP не було. Єдина відмінність полягала в тому, що протокол Modbus TCP забезпечував швидкість передачі даних на два-три порядки більшу, ніж протокол Modbus TCP.

Висновки

Для обміну даними між елементами систем автоматизації із невисокою швидкість можна рекомендувати протокол Modbus RTU, а із високою швидкістю – протокол Modbus TCP. По способу і надійності передачі даних ці обидва протоколи є приблизно однаковими.

ЛІТЕРАТУРА

1. Денисенко В. В. Компьютерное управление технологическим процессом, экспериментом, оборудованием [Текст] / В. В. Денисенко. – М. : Горячая линия-Телеком, 2009. – 608 с., ил.
2. Дианов В. Н. Диагностика и надёжность автоматических систем [Текст] / В. Н. Дианов. – М. : МГИУ, 2005. – 160 с.
3. Петров И. В. Программируемые контроллеры. Стандартные языки и приёмы прикладного программирования [Текст] / И. В. Петров / Под. ред. В. П. Дьяконова. – М. : СОЛОН Пресс, 2004. – 256 с.
4. Липаев В. В. Функциональная безопасность программных средств [Текст] / В. В. Липаев. – М. : Синтег, 2004. – 340 с.
5. Черкесов Г. Н. Надёжность аппаратно-программных комплексов [Текст] / Г. Н. Черкесов. – СПб. : Питер, 2005. – 479 с.
6. Александровская Л. Н., Афанасьев А. П., Лисов А. А. Современные методы обеспечения безотказности сложных технических систем [Текст] / Л. Н. Александровская, А. П. Афанасьев, А. А. Лисов. – М. : Логос, 2001. – 206 с.
7. Руководство по технологии объединённых сетей. 3-е изд. Пер. с англ. [Текст]. – М. : Издательский дом «Вильямс», 2002. – 1040 с.

© Київський національний університет технологій та дизайну, 2016

Применение коммуникационного протокола Modbus для обмена данными между элементами систем автоматизации

Лисовец С. Н., Коляда Д. М.

Киевский национальный университет технологий и дизайна

Рассмотрено обмен данными между элементами систем автоматизации, такими как ОВЕН ПЛК150, и персональным компьютером с автоматическим преобразователем интерфейсов ОВЕН USB/RS-485 АС4 и маршрутизатором TP-LINK 740n, по протоколам Modbus RTU и Modbus TCP. Установлено, что, кроме скорости обмена данными, оба протокола обеспечивают одинаковые функции для обмена данными и приблизительно одинаковую надёжность.

Ключевые слова: *ведомое устройство, ведущее устройство, кадр (фрейм), коммуникационный протокол, линия передачи, модули ввода/вывода, сетевой обмен, промышленная сеть, широковещательный режим*

The use of communication Modbus protocol for communication between the elements of automation systems

Lisovets S. N., Kolyada D. M.

Kyiv national university of technologies and design

Considered the exchange of data between the elements of automation systems, such as ОВЕН ПЛК150, and personal computer with automatic interface ОВЕН USB/RS-485 АС4 and router TP-LINK 740n, by protocols Modbus RTU and Modbus TCP. It is established that, in addition to the speed of data exchange, both protocols provide the same functions for data exchange and about the same reliability.

Keywords: *slave, master, frame, communication protocol, transmission line, modules input/output, network sharing, industrial network, broadcast mode*

© Київський національний університет технологій та дизайну, 2016