
A New Paradigm for Mixing RS-232, RS-485 & TCP/IP Ethernet in Multi-Vendor Automation Projects

RobustDC Application Note #28

Quick Index:

- ♦ The Growing Ethernet TCP/IP Challenge:
 - ♦ The Old Integration Paradigm - MODBUS/RTU over RS-232 or RS-485
 - ♦ The New Integration Paradigm - MODBUS/TCP over Ethernet TCP/IP
 - ♦ Example System Integrated with MODBUS/TCP over Ethernet TCP/IP
 - ♦ Summary
-
-

- **The Growing Ethernet TCP/IP Challenge:**

The use of robust Ethernet technologies - such as fiber optics, redundant media, and fast-switching/ATM hubs - is making Ethernet an increasingly popular industrial network back-bone. Either as part of the initial construction or as a later upgrade, end users are increasingly investing in a plant-wide Ethernet "utility" which includes access points in every area on site - possibly even to remote sites or neighboring countries! System integrators are seeing more and more quotations which include only Ethernet via sub-sea fiber optic cable to offshore platforms or Ethernet via high-speed leased lines to remote sites. Because this utility investment already exists, *small-to-medium sized integrators are increasingly being disadvantaged when quoting if they must include the cost of running additional copper or fiber optic or leased lines to support their Modbus or asynchronous serial communications.* We all know that the ability to integrate fully with the "big boys" is critical to the success of small-to-medium sized integrators and equipment makers. Therefore, the growing interest in Ethernet and TCP/IP is a trend to be monitored carefully.

So how can small companies add Ethernet TCP/IP support to their automation products without huge R&D budgets and long delays? Fortunately, there is a new paradigm developing which allows any device with MODBUS/RTU to instantly become a fully TCP/IP enabled device.

- **The Old "Integration Paradigm" - MODBUS/RTU over RS-232 or RS-485**

You've all heard of the MODBUS/RTU protocol. While MODBUS™ is a trademark of Schneider Automation, it is regarded as a "public" protocol and has become the de-facto standard in multi-vendor integration. MODBUS is a simple, flexible, publicly-published protocol which allows devices to exchange discrete and analog data. All end users know that specifying MODBUS/RTU as the required interface between sub-systems is the only sure way to achieve multi-vendor integration with the largest purchasing options and at the lowest cost. All small equipment makers know that they must offer MODBUS/RTU ports with RS-232 and/or RS-485 to have the easiest time selling their equipment to system integrators for use in these larger projects. All system integrators know that MODBUS/RTU is a safe interface to commit to, as they can be sure of finding enough equipment on the market to both realize the required designs - and handle the inevitable "change orders" which come along.

Yet MODBUS/RTU suffers increasing from the limitations of RS-232/485 serial lines:

1. Serial lines are relatively slow - 9600 to 115,000 baud means only 0.010Mbps to 0.115Mbps. Compare that to today's common "control network" speeds of 5 to 16Mbps - or even the new Ethernet speeds of 100Mbps and 1000Mbps!
2. While it is easy to link 2 or 3 devices by RS-232 and 20-30 devices by RS-485 - how do you link 500 devices with RS-232 and/or RS-485? The only solution is a complex hierarchy of masters and slaves in a deeply nested tree structure - these solutions are never "pretty" or easy to maintain!
3. Serial links with MODBUS/RTU are inherently "single-master" designs. That means, only one device can talk to a group of slave devices - so only that 1 master device can "know" what the current real-time data is. How can designers share this data with multiple operator workstations, control systems, data-base systems, customized process optimizing workstations, and all the other potential users of the data? Again, we end up with complex, fragile hierarchies of master/slave groups shuffling data "bucket-brigade" style up the ladder to all the potential users. Besides the complexity involved, lower levels of the hierarchy (even expensive DCS systems!) find themselves wasting valuable time shuffling data solely for the benefit of higher levels of the hierarchy.

• **The New "Integration Paradigm" - MODBUS/TCP over Ethernet TCP/IP**

Fortunately there is a new integration paradigm coming to the rescue of small-to-medium sized companies. MODBUS has quietly made the move to the world of mega-bits-per-second in the form of the MODBUS/TCP™ standard. While still a trademark & property of Schneider Automation, it is also publicly published and just as simple and flexible as the original Modbus/RTU standard. Modbus/TCP promises to become the de-facto standard for multi-vendor integration over TCP/IP networks.

Technically, MODBUS/TCP has been around a while - yet most people have neither heard of it nor been introduced to the absolute simplicity and brilliance of its use for multi-vendor TCP/IP networks. Modbus/TCP was introduced to support Modicon™ Quantum PLC with direct Ethernet adapters. Yet it is not an exotic, complex new protocol - merely MODBUS/RTU in a TCP/IP wrapper! So the real beauty of MODBUS/TCP is in how fast it can be implemented. *Any company with the following three (3) resources can implement MODBUS/TCP in a few days:*

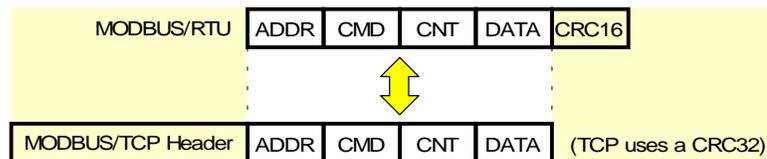


Figure 1) MODBUS/RTU to MODBUS/TCP Conversion

① source code for an existing MODBUS/RTU serial driver, ② a TCP socket library, and ③ one competent programmer. So presto, vendors can now have a MODBUS/TCP driver almost instantly, plus all their application programs which already support the data access paradigm of MODBUS/RTU can also support MODBUS/TCP just as easily.

So why call MODBUS/TCP the "TCP/IP Rescue Package"? Why do we need rescue from TCP/IP anyway? **The problem is that TCP is a transport protocol - not an user application protocol.** Saying 2 devices speak TCP/IP promises as much compatibility as saying they both have RS-232 ports! All TCP/IP does is allow blocks of binary data to be moved between computers - it does not help you interpret what that data

means! It is 100% analogous to the postal system. I can received a letter posted from Japan or Pakistan and addressed perfectly to me - both you and I fully support the "snail-mail postal system protocol"! Yet the postal system cannot help me read the letter inside if it is written in Japanese or Arabic, can it! In the same manner as the postal system, TCP/IP safely moves blocks of data between 2 different systems. TCP/IP handles blocks of any size, whether 10 or 100 or even 1,000,000 bytes, but TCP/IP can promise absolutely nothing about what that data means or how to interpret it. There still has to be agreed upon rules to interpret that data - a user application protocol like MODBUS/TCP. (For details of the MODBUS/TCP specification see <http://www.modicon.com/openmbus> and for information on multi-vendor availability see http://www.robustdc.com/mbus_tcp.htm)

• **Example System Integrated with MODBUS/TCP over TCP/IP**

Figure 2 shows a simple multi-vendor system integrated with MODBUS/TCP. It also introduces the idea of a protocol bridge (PB) to integrate older RS-232 and RS-485 MODBUS/RTU and MODBUS/ASCII devices into a new TCP/IP network. These devices are already available from a number of companies - search the Web for "Modbus TCP" to find some of them. This example shows 3 work-stations from 2 different vendors and 5

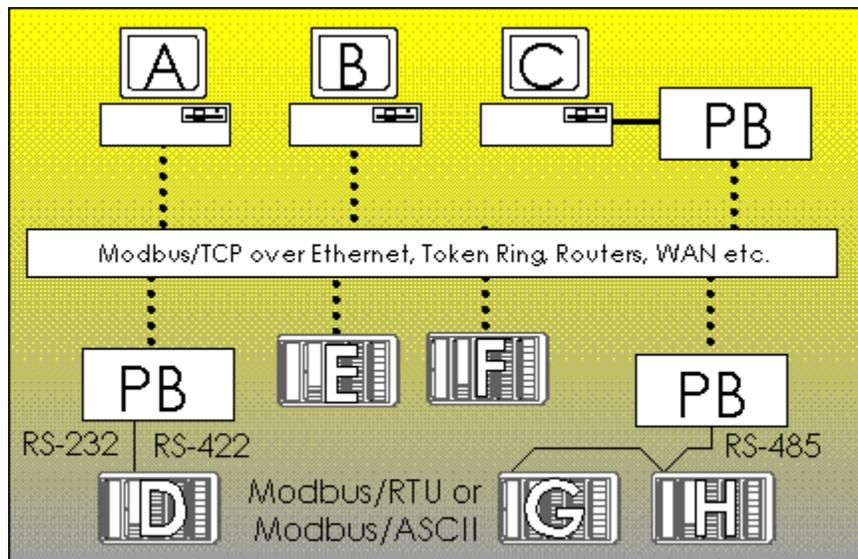


Figure 2) TCP/IP Integrated System

field devices from 3 different vendors. The TCP/IP Ethernet acts as the "mixing medium" allowing them all to talk freely between themselves. In this design, A, B, C, E, and F can all act as MODBUS masters, while D, E, F, G, & H can act as MODBUS slaves.

Starting at the top, **Workstations A and B** use standard MMI software. Most commercially available packages already support MODBUS/TCP - ask for their "Modicon Ethernet Quantum PLC" servers as many supplier don't realize these are really MODBUS/TCP drivers! Remarkably, both A and B can act as masters to all field devices D through H. Surprised? Even if devices D, G, & H only have 1 serial port each, both A and B can act concurrently as MODBUS masters to them! (Honest, it works!) **Workstation C** is a special DOS-based programming and monitoring station for field devices G & H. Since this vendor only supports MODBUS/RTU over normal COM ports, the protocol bridge (PB) is used to integrate C into the MODBUS/TCP system. Notice how the inherent multi-access nature of TCP/IP and MODBUS/TCP allows all three workstations to share being Master to all 5 field devices!

Now for the field devices: **Field device D** is an older device which only supports MODBUS/ASCII with an RS-232 port. Not only does the protocol bridge (PB) convert the MODBUS/ASCII to MODBUS/TCP, but even workstation C - which only supports MODBUS/RTU - can now access field device D. The PB allows this transparently support even this RTU to ASCII conversion. **Field devices E & F** are newer products with direct Ethernet and MODBUS/TCP support. **Field devices G & H** support MODBUS/RTU over RS-485.

But we are not finished yet. Direct MODBUS/TCP support means field devices E & F can be both MODBUS master and MODBUS slave devices at the same time. Not only can they provide data requested by masters A, B, & C, but they can use their own "master functions" to pull data directly from field devices D, G & H. Remember, field device D only speaks MODBUS/ASCII, field device E & F only speak MODBUS/TCP, and field devices G & H only speak MODBUS/RTU. The clever design of the new MODBUS/TCP protocol and the flexibility of the old MODBUS/RTU and MODBUS/ASCII protocols allow compatibility and conversation between all three.

- **Summary**

All local automation professionals should search out and become familiar with the latest Ethernet and TCP/IP technologies. Then they will be ready to profit from application of these new technologies and the more flexible multi-vendor systems they enable. We already know of several small local companies who beat out the competition by proposing state-of-the-art Modbus TCP/IP solutions for the same money as their competitors tried to sell "old-fashioned" serial solutions. Don't let these opportunities pass you by.

1. Buy a book on the subject of TCP/IP - titles like the "Dummies Guide to TCP/IP" readily exist at all good book-shops. These will explain IP and UDP and TCP and FTP and all the other acronyms and jargon you need to "talk the talk" and make the sale.
2. Review the MODBUS/TCP specification at www.modicon.com/openmbus
3. Ask your software application suppliers for MODBUS/TCP drivers and servers. If they don't have them yet, press them to spend those **few days** to create them so you are ready when opportunity knocks. It's the best "few days" you or they will ever spend!
4. Locate sources for Modbus protocol bridges through the Web and at upcoming trade shows. These allow you to sell your existing Modbus/RTU solutions in new TCP/IP systems.
5. Make contact with local IT and networking suppliers to learn how to design and implement robust Ethernet designs including redundant media and fiber optics support. DIN-rail mount and 24vdc supply models are even available.

- **For More Information**

Robust DataComm can truly make your data flow like water - safely, sanely, and silently.

Robust DataComm
26471 Portola Pkway, Suite 1E-242
Foothill Ranch, CA 92610-1743 U.S.A.
US Sales: (972)248-7466 Fax: (972)248-9533
email : info@robustdc.com

Robust DataComm Pte Ltd
18 Kaki Bukit Road 3 #02-08
Entrepreneur Business Center Singapore 415978
Tel: (65)6487-5624 Fax: (65)6288-3306
web : <http://www.robustdc.com>

Copyright © 1993-2001 Robust DataComm, USA and Singapore, All Rights Reserved.