

Spring 2010

Modbus Organization Releases Toolkit v3.0

In February, the Modbus Organization released version 3.0 of the Modbus TCP Toolkit. This new version replaces version 2.1 and includes some new resources for developers seeking to implement Modbus. These include an updated test tool, Modbus Conformance Test Tool v3.0 (and accompanying updated test specification), and various other resources for implementation and device testing. Use of these resources speeds development and allows developers to prepare for conformance testing at a certified Modbus Organization Conformance Test Lab.

The upgraded conformance test tool provides broader test coverage with more flexible configuration to test nearly any memory architecture. Developers can test specific function codes or run the full test suite. Each test sequence is logged for post-test evaluation.

The new test tool is now being used in the Modbus Organization's Device Certification Program, available to all suppliers. Modbus member companies participating in the Modbus Organization's self-testing program have also switched to the new test tool.

Special thanks for contributed projects and committee work go to Control Solutions, Eaton Corporation, and Triangle MicroWorks.

New Open-Source Modbus Implementations

Two new open-source applications have been listed on the Modbus Technical Resources page (www.modbus.org/tech.php):

- **Modbus4J** — a high-performance and easy-to-use implementation of the Modbus protocol written in Java by Serotonin Software. This implementation supports Modbus ASCII, RTU, TCP, and UDP transport as slave or master, and supports automatic request partitioning, response data type parsing, and node scanning.
- **Mango M2M** — This browser-based, Ajax-enabled M2M software enables users to access and control electronic sensors, devices, and machines over multiple protocols (including Modbus) simultaneously. Diverse data sources can be created and configured while providing downstream management of user access, alerts, data logging, and automation.

Are You Going to Hannover Fair?

Looking for suppliers of Modbus devices or Modbus expertise at the fair? Many Modbus Organization member companies are exhibiting at Hannover this year. For your convenience, here are the locations of those members that will be there:



- **connectBlue:** Hall 7, Stand A46
- **Control Techniques:** Hall 15, Stand H35
- **Danfoss:** Hall 9, Stand D68
- **Eaton:** Hall 11, Stand C69
- **EWON:** Hall 7, Stand D46
- **Fieldbus International:** Hall 7, Stand B09
- **Hilscher:** Hall 11, Stand A62
- **Hirschmann Automation & Control:** Hall 7, Stand A46
- **HMS Industrial Networks:** Hall 9, Stand D18
- **Klaxon Signals:** Hall 8, Stand B15
- **Phoenix Contact:** Hall 9, Stand F40
- **Softing:** Hall 7, Stand B09
- **Schneider Electric:** Hall 11, Stand B39
- **Wachendorff Prozesstechnik:** Hall 7, Stand A46

More Choices for Wireless Modbus Communication

With increasing demand for wireless communications in industrial settings, suppliers are responding by equipping their devices with wireless capabilities. Three Modbus member companies announced the release of new devices to meet this demand over the past couple of months.

Read about the Hach Company's sc1000 Multi-Parameter Controller with built-in GPRS modem, ProSoft's Industrial Hotspot™ radios, and Phoenix Contact's busable 900-MHz radio on pages 5 and 6.



Many more wireless devices are listed in the Modbus Device Directory (www.modbus.org/devices.php). Simply filter on "Wireless Devices Only" to locate the right Modbus wireless device for your project.

Meet Some of Our Members...



With annual production of more than 16 million pump units, **Grundfos** is one of the world's leading pump manufacturers. Circulator pumps for heating and air-conditioning and other centrifugal pumps for industry, water supply, waste water, and dosing are the company's major products. Today, Grundfos has approximately 50 percent of the world market for circulator pumps.

In addition to pumps, Grundfos manufactures norm and submersible motors for its pumps (the motors are also available as separate merchandise), as well as electronics for monitoring, controls for pumps and other systems, and the products BioBooster and NoNox, which are part of the company's new business activities.

Established in 1945, Grundfos Group Management is located in Bjerringbro, Denmark.

(www.grundfos.com)

Shouldn't your company
be a member?



Headquartered in Birkerød, Denmark, **JVL Industri Elektronik A/S** focuses on its core business — motor control systems.

JVL first gained its reputation in the 1980s for the development of modern, compact step-motor drivers and controllers.



In the 1990s this was followed by development of a series of second-to-none AC and DC servo controllers, which led to marketing of the unique integrated AC servo motor, the MAC motor, (up to 734W), and the QuickStep, integrated stepper motor (up to 2.9Nm) which both include the entire controller, encoder, etc. in one compact unit.

The latest firmware for the integrated servo motors MAC400 and MAC800 now supports Modbus RTU.

The implementation supports the Read Holding Registers and Write Multiple Registers commands, gives R/W access to all motor registers at speeds up to one Mbps.

The firmware supports two-wire RS-485, as well as both four-wire RS-485 and RS-422 standards.

(www.jvl.dk)

Hach Company provides the widest digital communication capability in the world of continuous sensors and controllers for water and waste water analysis. These sensors help with secure, efficient operation of treatment plants as well as other industrial applications. They can be integrated easily into common PLC, OPC, and SCADA systems using Modbus RTU and Modbus TCP — even for wireless applications, using a built-in GPRS module as the transport layer for global communication.

Hach's offerings include its MOD I/O Modbus Interface, a cost-effective solution for analog-to-digital communication. The MOD I/O comes with a power supply, RS-232 cable, and a manual. Using Modbus ensures compatibility with virtually all PLC/SCADA systems. MOD I/O can be used with all Hach AquaTrend water analysis instruments.



The Modbus Organization Mission

The Modbus Organization, Inc. is a group of independent users and suppliers of automation devices that seeks to drive the adoption of the Modbus communication protocol suite and the evolution to address architectures for distributed automation systems across multiple market segments. Modbus Organization also provides the infrastructure to obtain and share information about the protocols, their application, and certification to simplify implementation by users resulting in reduced costs.

Modbus Newsletter

This is the newsletter of the Modbus Organization, the international non-profit organization devoted to the evolution and support of the Modbus protocols. For more information about membership and other services, please refer to our website: www.modbus.org

Newsletter Editor:

Lenore Tracey (lenore@modbus.org)

Copyright 2009 by the Modbus Organization, Inc.

PO Box 628

Hopkinton, MA 01748 USA

ph +1-508-435-7170

fax +1-508-435-7172

info@modbus.org

Modbus Discussion

Q&A

From the Modbus Discussion Forum...

Modbus/TCP and inetd?...

In December, Ian Goldby wrote:

I'm wondering if it is sensible to write a Modbus TCP server as an inetd child process. In many ways this simplifies the server, because it has to deal only with one client at a time and all I/O is piped through stdin and stdout (no sockets programming).

But I wonder if many Modbus clients open and close a connection each time they make a request. With inetd there is something of a performance penalty when a new connection is opened, because inetd has to fork a new instance of the server process each time.

A Google search for "Modbus inetd" returns nothing that seems relevant.

Does anyone have any relevant experience they can offer?

M. Griffin explained:

It's normal for a client to hold the socket open unless some major error forces it to close. The reason of course is to avoid overhead when polling at a fast rate.

The exception to this is when the client is polling very slowly, in which case it may close the socket as soon as it is done. In some applications the client might only poll once per hour or even once per day, in which case there is no point in leaving the socket open. In that case, the extra overhead of opening the

connection isn't typically going to be a problem.

The server needs to deal with multiple simultaneous connections, but they all need to go back to a common data table. A forking server would probably work just fine. I don't know if it has been done before. If it hasn't, it's probably because in most designs the server is part of the application program.

If you made the Modbus server a separate server and the application program (the thing that is going to actually do something interesting) could talk to it via some other fairly simple means (e.g., via a UNIX socket) then that would probably be useful. The Modbus server could run as a privileged program on port 502, while the application program could talk to it without having to worry about setuid.

I've written several Python programs which have Modbus TCP servers integrated into them. MS Windows, has no security protection for "well known" server ports, so they could use port 502 directly there. For Linux, the solution that I came up with was to run the program on a higher port and use iptables to redirect 502 to that port. That meant I didn't have to deal with making sure that I was handling all the security implications correctly, since the program runs at a normal user level at all times.

<http://sourceforge.net/projects/mblogic/>

A Modbus TCP server that ran as a separate component wouldn't have to deal with that, and so would be a useful way of adding server capabilities to programs.

Tallak Tveide added:

From what I've seen I would expect close to all clients doing periodic requests on a single TCP/IP connection. The overhead in question should be no big deal :-)

You could see for yourself with Wireshark — each connection will be shown clearly.

Read the rest of this discussion and add your comments to this thread at modbus.control.com/thread/1260976781.

Need a Modbus Device for Your Project?

Search the database at www.modbus.org/devices.php to find the right Modbus device for your application.



Modbus Discussion

Q&A

More from the Modbus Discussion Forum...

Modbus Master to Master...

In February, Santi posed the following question:

If an intelligent device (PLC) is only configurable like a Modbus master, can I query this from a PC application (e.g., SCADA)?

Russ Bartels answered:

Maybe. Some Modbus master devices will reply to standard “slave” requests from another master on the same bus. Just remember that they need different node addresses.

You should check with the PLC manufacturer.

From M. Griffin:

Like most protocols, Modbus is a client/server (or master/slave) protocol. The client (master) sends a query, and the server (slave) responds to it. It’s just like the way your web browser (client) communicates with Control.com (server).

If the SCADA can be a server and the PLC is a client, then the PLC can talk to it. If the SCADA and the PLC both insist on being clients (masters), then the solution is to put a “proxy server” in between them. The proxy acts as server to both parties. The PLC would write to the proxy, and the SCADA would read from it (and vice versa).

If you are dealing with Modbus TCP on Ethernet (as opposed to an RS-485 Modbus), then any station can be both a client and a server simultaneously *provided* its software was written to support this. This is not typical for PLCs (they are usually one or the other). For the SCADA you would have to look into what its drivers are capable of.

Ian Goldby did not agree:

No, you can’t. Not directly anyway.

The fundamental problem is that a Modbus master does not respond to unsolicited requests. There is no such thing as this in the Modbus protocol.

The only way a Modbus master can get information is by asking for it.

Conversely, a slave deals only with unsolicited requests. It cannot send a message unbidden.

The second problem is that Modbus is fundamentally a master/slave protocol. There is no peer-to-peer in Modbus.

Patrick Lansdorf suggested the following approach:

You will need a gateway that is a Modbus RTU slave to Modbus RTU slave, such as the Anybus X-gateway.

With it you will be able to share data between two Modbus RTU masters, pretty much like a DP/DP coupler for Profibus.

Fred Loveless offered another possible solution:

I have never seen it done yet, but that does not mean it cannot be [done] if the devices support it. If you need to get data from the master device into a SCADA and from the SCADA back to master, use an OPC or DDE Server that can be configured to be a Modbus slave on the network. Then the master PLC can Read and Write to the slave device, and your SCADA is updated from the slave server and can write down to it so that the value can be polled by the master.

Mike Lamond had another idea:

I know of one case where a Modbus port can be both slave and master, but not at the same time, of course. In Modicon Quantum, Momentum, TSX Compact and some Micro 984 models, the XMIT 984 loadable and the Concept IEC XMIT function take control of a Modbus port to act as a master device. When XMIT is not active, the port reverts to its configured slave setting.

We used this on a radio telemetry project to make one site a data repeater for another site that was blocked from

the master radio by a hill. There are extra flags programmed so that the repeater site waits as a Modbus slave until it receives permission from the master site, after which it becomes a Modbus master and the master site acts as a Modbus slave. Once finished, the repeater returns permission to the master site and the cycle continues.

I haven’t had any experience with the newer Schneider PLCs and software, so I don’t know if this technique has become obsolete.

Robert Willis confirmed this:

The XXMIT Function block would allow the Modbus Port (Port 1) to be used as either a master or a slave. Once the XXMIT “master” message is completed, the port would revert back to the slave configuration. The arbitration between master and slave would need to be worked out by the developer so that both the local and remote can communicate.

You also might want to look at the NR&D products that have a Modbus Gate Mode setting for serial ports. This allows the serial port to automatically transition between a master or slave configuration depending on the message source.

Modbus users & suppliers get together on the Modbus Community for:

- Interactivity
- Knowledge aggregation
- Contact with Modbus users and suppliers

Discussion supported by...



Modbus Discussion

From Gustavo A. Valero P.:

Going back to the initial question written by Santi, the answer is YES but it depends on the SCADA's driver.

Some drivers support something called "Unsolicited Read," and with this feature you can get what you want, e.g., most FactoryLink drivers support "Unsolicited Read" feature including its Modbus TCP driver.

This driver opens three threads/connections to the NOE module of PLC (was developed to work with Quantum PLCs originally). One thread/connection is required for each of the following operations: Reads, Writes, and Unsolicited Reads. These threads must be available even if these operations are not configured in the application.

At its beginning, if a PLC that claimed to support Modbus TCP protocol was not able to support these three connections, the driver was not going to work with the PLC, but after some modifications and improvements, this issue was eliminated.

Unfortunately, the driver only works and waits for Unsolicited Reads based on Holding Registers (HREG)... nothing is perfect!

Your plan B could be to use an I/O Gateway device able to work as master/slave Modbus at the same time and exchange data between the masters

using the Gateway's internal/virtual memory as a "bridge." I have used this solution before with [SIXNET] equipment perfectly.

JMW :

This thread is very fortuitous for me as I have been puzzling over a similar problem.

I have two transmitters that normally would both be slaves multi-dropped to a master controller.. However, I have an application where I need these two transmitters to share information with each other, perform similar calculations, and then output the results.

So to share information one or the other or both would have to be able to solicit data from the other and both respond to an external data call from the master controller.

Effectively this means three masters... or am I wrong?

It would be neat and tidy if the true master were to poll data from both slaves and then send data collected from one slave to the other slave, but I also have the possibility that in some applications there will be just the two transmitters and the "master" controller would only accept 4-20mA data so the two slaves will have to do it all themselves.

I just need a heads up on feasibility for now, thanks.

M Griffin replied:

A device could be a client (master) or server (slave). In some cases it is possible to be both at the same time. It is up to the device designer to decide what features and functions make sense for that application and then to implement those features. Modbus specifies what the message format looks like. It doesn't (with a few exceptions) specify how your device works. As long as the messages which go out on the wire conform to the format in the Modbus specifications, it's still Modbus.

You will find the same is true for many (if not most) other protocols. There are a lot of features in many protocols that are intended for certain narrow applications, and which have no value in other applications. The designers then just implement subsets of the full protocol. With proprietary protocols, however, they very rarely tell you what is really going on under the lid, so it may not be as obvious as to what the limitations are.

Read the whole thread & add your thoughts at modbus.control.com/thread/1265915114

Hach Liquid Analysis Portfolio Goes Modbus TCP Wired and Wireless

The Hach Model sc1000 Multi-Parameter Controller is now available with state-of-the-art Modbus TCP communication protocols and a built-in GPRS modem for seamless integration into corporate internet and MES systems. Using Modbus TCP, system data can now be transmitted over an Ethernet physical layer or streamed wirelessly using GPRS around the globe.

System data that is stored in the sc1000 can also be accessed using an on-board web server. The enhancements in the sc1000's digital communications capability enable customers to integrate the sc1000 controller easily into their networks as well as save them money by reducing wiring and cabling costs. Up to five Modbus masters are supported simultaneously while parameterization, configuration, and diagnostics can be performed using any browser.

For more information, visit www.hach.com.



**Hach Company's
sc1000**

Modbus Products and Innovations

ProSoft's New 802.11 Industrial Hotspot™ Radios

Industrial Hotspot™ solutions provide excellent connectivity to customers using Modbus TCP in their control systems. They provide premier performance for high-capacity networks and offer a wireless solution for applications with moving or obstructed environments, which are traditionally difficult to address with wireless technology. The 5-GHz band gives users another 23 channels that can operate simultaneously without conflicting with pre-existing wireless applications operating on the 2.4-GHz band.

The RLXIB-IHxN series of radios is optimized for rugged industrial performance and easy deployment in the field using a single webpage setup. Reliable I/O message delivery, industrial temperature range and hazardous location ratings, as well as RADIUS security for centralized management of security policies, VLANs for network traffic segmentation, and Quality of Service (QoS) for data prioritization and dual radio functionality round out the feature set.

The 802.11n Industrial Hotspots improve performance for high-bandwidth video/voice applications and high packet-rate control applications. Available options include the Single (RLXIB-IHN), Dual (RLXIB-IH2N), and Watertight Dual (RLXIB-IH2N-W) versions.

The radios take advantage of MIMO (Multiple Input, Multiple Output) — a technology that uses up to three antennas to enable data rates up to 300 Mbps. In addition, this series of radios actually provides two radios in one and only requires a single Ethernet connection. Dual radios can be used in lieu of a repeater to extend the range of the wireless network without sacrificing speed.



The RLXIB-IHN includes the industrial features of other RadioLinx products, including hazardous location certifications (UL1604 Class I Div 2, ATEX Zone 2 Category 3), extended operating temperature range, high vibration/shock resistance, DIN-rail mounting, Power over Ethernet and simultaneous bridge/repeater/access point mode.

Harry Forbes of ARC Advisory Group commented, “These new ProSoft Hotspots are among the first to bring 802.11n technology to industrial automation networks. IEEE 802.11n brings a higher level of wireless performance to plant floor applications. Also, MIMO technology reduces the multipath interference that is common in industrial installations.”

For more information, visit www.prosoft-technology.com.



ProSoft's 802.11 Industrial Hotspot Radios

Phoenix Contact Releases Busable 900-MHz Radio for Simple I/O Data Connection

A busable 900 MHz radio is the newest addition to Phoenix Contact's Trusted Wireless Ethernet (TWE) portfolio of industrial wireless products. The RAD-ISM-900-EN-BUS allows direct connection of I/O modules to the radio.



Phoenix Contact's RAD-ISM-900-EN-BUS

The radio allows the user to collect I/O without a remotely located PLC or I/O data concentrator. The bused I/O is made accessible to the network using the readily available Modbus protocol. It can easily be integrated into new or existing PLC, SCADA, or DCS systems.

Phoenix Contact has also added a multiple master function to the 900 MHz TWE radio family. This function can create redundancy and wireless failover connections if a master or host radio is not accessible. The new multiple master function and busable radio make the 900-MHz TWE radios ideal for a variety of industrial applications such as tank level, pressure, and temperature monitoring, pump status and control, and SCADA system expansion.

For more information on the industrial wireless radios or any Phoenix Contact product, visit www.phoenixcontact.com.



Join! Design! Test! Promote! Apply!

We're with you. The Modbus Organization exists to help suppliers and users of Modbus protocols succeed. Our members range from suppliers of Modbus-compliant products, to system integrators, end users, and educational institutions.

The common link? They all value the information and services provided by the Modbus Organization, and they all play a role in determining the future of the world's most broadly applied protocol.

To join the Modbus Organization, order a Toolkit, or arrange conformance testing, visit our website:

modbus.org

Designing with Modbus

Each day, Modbus developers turn to the Modbus Organization for valued assistance with their projects:

- Start with downloading specifications and other design documents from the modbus-ida.org website.
- To really save time, purchase the Modbus TCP Toolkit CD (FREE with general membership); it contains source code and a myriad of other resources.
- Then, if you come across technical issues that have you stumped, post your question on our active developer's forum. One of the many experienced Modbus implementers who frequent this forum will likely have your answer.

Conformance Testing

When your project's done, what then? How do you know it really conforms to Modbus specifications? How do your users know?

The answer starts with running the conformance test suite included with your Modbus TCP Toolkit. This self-

test helps you check your design assumptions and catch the subtle "gotchas" that might otherwise slip through your design review.

To make the definitive statement of your company's commitment to open protocols, submit your product for testing to the independent Modbus Organization Conformance Test Lab. We'll certify your product as compliant, and post that information on the Modbus website for the world to see.

Visibility: Your Company & Your Products

Your membership in the Modbus Organization also opens the door to a powerful range of visibility options to highlight your company as a supplier of Modbus-based products.

Exposure on our website, our newsletter, and through our various trade show appearances are all options that allow you to make the most of your Modbus Organization membership.

If your company is truly on the cutting edge of new technology, you'll likely also value the opportunity to participate in our technical committees. There, your company's knowledge, experience and technology can help guide future enhancements, extensions and adaptations of Modbus to keep it the world's leader for decades to come.

Time to Apply

When it comes time to get your Modbus network up and running, it's comforting to know that hundreds of thousands of applications have preceded yours. But what if things don't go as planned?

The modbus.org users forum is ready to answer your questions and provide guidance. Thousands of users from diverse backgrounds read the forum, giving you a powerful base of experience from which to draw.

The Future is Yours

So, whatever your role in the use of Modbus, consider joining the Modbus Organization. You'll get the support you need today, and have opportunities to help guide Modbus to a dynamic future.

Modbus TCP Toolkit v3.0

The Modbus TCP Toolkit provides all the necessary pieces to develop a Modbus-compliant device, including documentation, diagnostic tools, sample source code, and pre-test software to prepare for Modbus conformance certification. The toolkit is available as a benefit of corporate-level membership in the Modbus Organization or can be purchased separately for US\$500 plus shipping and handling.



Toolkit Contents

Modbus Documentation

- Modbus Application Protocol Specification, v1.1b
- Modbus Messaging on TCP Implementation Guide, v1.0b

Tools

- Modbus TCP Client and Server Diagnostic Tools

Sample Source Code

- Modbus TCP Sample Client Code for Visual Basic Win32
- Modbus TCP Sample Client Code for C/C++ Win32
- Modbus TCP Sample Server Code for C/C++ Win32
- Modbus TCP Sample Server Code for C VxWorks
- Modbus TCP Sample Server Code for C++ VxWorks

Conformance Testing

- Modbus Conformance Test Tool v3.0
- Modbus Conformance Test Tool v2.1

Additional Resources