

New Open-Source Modbus Implementation

A new open-source applications has been listed on the [Modbus Technical Resources](#) page:

- **RModbus** — a free Ruby implementation of the Modbus protocol. It supports Modbus RTU and Modbus TCP as master or slave. For the extensive list of all currently supported features please refer to the project web site.

Busy Summer for Modbus Member Companies

It's been a productive summer for Modbus Organization member companies. Here is a sampling of the new Modbus products that came out recently:

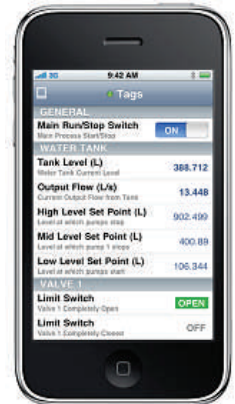
- **Control** released Modbus Server firmware
- **SCADAmetrics** announced the addition of the new TRF-W to its line of meter-reading devices
- **Danfoss** released the VLT® Soft Starter MCD 500
- **Acromag** is offering ActiveX and .NET controls for its Modbus TCP and RTU I/O Modules

Visit Modbus.org to learn more.



ProSoft's New Modbus iPhone Application

[ProSoft Technology](#) announced the support of the Industrial Hotspot series of radios in conjunction with Sweet William Automation's new ScadaMobile application for the iPhone/iPod platform. The application provides engineers with access to live process control variables, and the ability to modify this data remotely from their iPhones.



The app. creates a secure wireless interface between an iPhone and an existing 802.11 wireless network on the plant-floor, allowing the iPhone device to read Modbus TCP and EtherNet/IP process control variables from programmable automation controllers/programmable logic controllers (PAC/PLCs) distributed throughout the plant. Live values are displayed in lists and include user-defined variance allowances and alarms. Engineers can monitor these variables in real time and make adjustments on the fly from an iPhone.

The combined security features offered by the iPhone and ProSoft's Industrial Hotspot radios prevent unauthorized access to the network. ProSoft's new 802.11n industrial hotspots feature WPA2-PSK and 802.11i RADIUS security, which prevent unauthorized access and modification to the network. ScadaMobile also provides a security feature upon configuration that requires the user to assign a matching security code as both a password for network access and as a Security Tag in the CPU. When ScadaMobile launches, the security code must match that on the CPU in order to create a connection.

continued on page 4

Deep Sea Electronics

Established in 1975, Deep Sea Electronics has over thirty years experience in creating market-leading generator controllers. DSE has a comprehensive range of products, specializing in automatic start generator controllers, automatic mains failure controllers, and auto transfer switch controllers. DSE has a technologically advanced collection of load share and electronic engine compatible solutions.



® All products are manufactured on-site at the company's headquarters in the UK. DSE has an

additional office in North America, as well as a comprehensive global distributor network.

DSE has incorporated Modbus RTU into its product line.

California-based Actel Corporation is a leader in low-power Field-Programmable Gate Arrays (FPGAs) and mixed-signal FPGAs. The company offers a comprehensive portfolio of system and power management solutions.



Actel implements interface standards in its products, including Modbus, PROFIBUS, WorldFIP, and P-NET.

The company's products are used in LCD control signal generation, battery management, industrial and medical equipment, and military and aerospace applications around the world.

Frontline Test Equipment is a leading provider of PC-based protocol analyzers for special-purpose data communication networks. Frontline pioneered portable and versatile trouble-



shooting software solutions for serial and Ethernet network topologies and communication protocols.

The growing family of Frontline Test System (FTS) general-purpose and industry-specific protocol analyzers is based on a common protocol-decoding engine. FTS products provide a common user interface, offer protocol decoding at the bit level, and enable the rapid development of custom decodes for proprietary protocols and extensions to existing protocol decoders. Frontline's Modbus-related products include Serialtest® and NetDecoder(TM).



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 nonprofit 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 2010
Modbus Organization, Inc.

Saving the Famous Bellagio Las Vegas Water Fountains from Extinction

Dancing water is the signature trademark of the Bellagio Hotel, and last year it became clear that keeping the water show running might require a major investment in an entire new control system. The original system was built around several hundred pumps driven by obsolete Danfoss 2200 drives using a proprietary protocol. The Bellagio avoided a major investment by using a **Real Time Automation** gateway to interface Rockwell Automation POWERFLEX drives with the legacy water fountain control system.

In early 2009 it became clear that the dancing water show at the Bellagio Hotel, one of the most renowned attractions on the Las Vegas strip, was in peril due to the obsolescence of the Danfoss 2200 drives used to build it in 1998.

The Bellagio was created to be the pinnacle of opulence. Modeled after the extravagant Lake Como Resort in Bellagio Italy, the Las Vegas Bellagio is a must-see for every visitor.

With over 200 fountains, the Bellagio fountain show is considered the largest and most technologically advanced show of its kind in the world.

The fountains are literally an oasis in the desert. Fed by a well once used to water the Dunes Golf Course, which used to reside on the same grounds, the fountains use only 10% of the water the golf course once used.

The fountains are powered by 220 pump houses located at the bottom of the eight-acre lake.



The obsolete Danfoss 2200 drives power pumps that send some of the over 1,200 streams of water as high as 460 feet in the air.

Over the years, the engineers at the Bellagio scoured the globe gathering all the 2200 drives they could find, but by early 2009 it was clear that the supply was simply running dry. Without a replacement for the drives, the show would soon come to a halt. To make matters worse, the economic recession had left Los Vegas in a deep freeze as the number of visitors to Sin City plummeted. A low-cost replacement option was needed to keep the fountains up and running.

The possibility of simply replacing the drives with more current drives was quickly discarded. Any other drive would have a different communication protocol, necessitating major changes to the water show's hardware and/or software system. That would be high risk and expensive, as extensive time and testing would be required. Plus there would be no mechanism to phase in a few at a time. The entire show would have to go dark while all drives and software were updated.

Instead, Real Time Automation proposed a solution based on an existing RTA gateway product. RTA proposed customizing one of its gateways to emulate the defunct drive so that none of the show control software or hardware would require modification.

Real Time Automation created a solution that talked Modbus RTU over an RS-232 port to a Rockwell Automation POWERFLEX drive, while communicating with the legacy water fountain control system using the DF2200 drive's proprietary serial protocol.

Using this module the Bellagio solution was delivered within days and functioned nearly perfectly during commissioning and dry testing on land. The custom protocol and logic for the DF2200 drive was added directly on top of the established and tested Modbus RTU code. This led to a much shorter testing period and very rapid advancement from beta to production. The gateway module made the POWERFLEX drive appear to be a Danfoss 2200 drive, allowing seamless and efficient integration — a true plug and play replacement solution.

continued on page 4

cont'd from pg 1

cont'd from pg 3

Modbus iPhone App.

By using the ScadaMobile application in conjunction with ProSoft Technology's Industrial Hotspot series of radios, engineers can manage their industrial processes remotely. The Industrial Hotspots are certified for hazardous environments and optimized for plant-wide network integration, particularly the new 802.11n series, which is designed to meet the specific needs of industrial customers who demand ease of deployment, ruggedness, and reliable industrial communication.

For plant engineers, this solution enables:

- Live monitoring of process data for engineers and plant floor operators
- Secure remote monitoring and modification of live process data
- Real-time alarm management

Bellagio Fountains

Once testing was completed on land, the solution had to perform under water. Installation in this environment was a daunting three-day task.

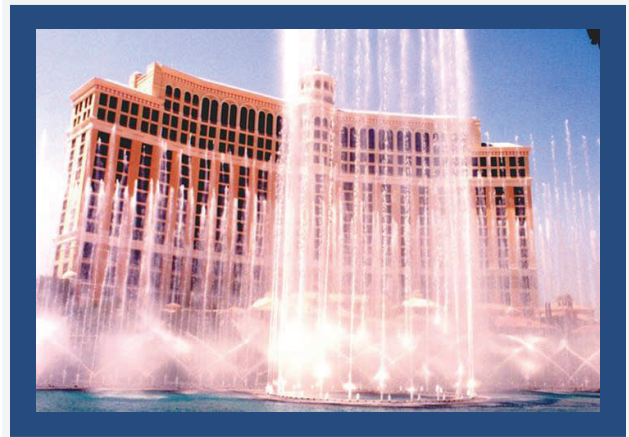
First divers dove to the bottom of Lake Bellagio to disconnect the pump platform from its power and network connections.

Then a small crane was floated over and the 15' high structure was lifted out of the water and onto a raft. After it was moved inside the facility, the platform was given 24 hours to dry.

Once dry, the drive solution was installed and tested. Finally the unit was sealed, moved back, lowered into the lake, and connected to power and the show controller.

With shows as often as 15 minutes a day, one day of testing confirmed that the solution saved the dancing waters from extinction.

Real Time Automation supplies EtherNet/IP, Modbus TCP, Modbus RTU and DeviceNet gateways to system integrators and end users around the world. RTA also tailors these gateways for specific applications like the Bellagio Fountains. For more information on the company's many Modbus gateways or for information on tailored applications like this, please visit the [Real Time Automation's website](#).



Modbus humor courtesy of our friends at [Automation.com](#)



Be Right™



AFCON SOFTWARE AND ELECTRONICS LTD.



Q&A from the Modbus Discussion Forum...

Most used Modbus Functions...

Luca Gallina wrote to the forum:

I am developing a software Modbus driver for S7-300/-400 PLCs, getting rid of expensive CP341/441 and their external loadable drivers.

My personal experience on a few cases tells me that almost no real field applications require access to memory area others than registers 30001.. and 40001.. (Most requests are instrumentation and DCS interfacing).

I am therefore focusing only on Modbus functions FC03, FC04, FC06 and FC16.

My question: In your real world applications do you often (or never) need to access Modbus functions other than the ones I listed above?

M Griffin replied:

I think it depends on the application. If you are logging production data then it's usually just registers. However, if you are dealing with a simple HMI or reporting status (is the machine in auto, are there any faults, etc.), then coils and (to a lesser extent) discrete inputs get used a lot.

If the software on the other end is flexible, then it might be able to use data in registers rather than coils. However, some software insists on having coils for some functionality. That would mean 1, 2, 5, and 15.

On the other hand, having register-only access is still better than having none at all.

Will you be doing a TCP version as well as RTU? I'm assuming this is RTU as you mentioned a CP341.

Harvard offered:

[Function] codes 1, 2, and 5 are also a common offering on any generic host. IMO.

Lynn August Linse suggested:

The other replies are good — but I would avoid FC04. Some common client/hosts cannot issue FC04 requests.

The bit functions FC01 and FC02 can be complex to create in a language without shifts, because literally you can read the 3rd to 6th bits, which must be shifted over 3 places to return as-if the 1st to 3rd bits of a byte.

So I'd suggest:

- 1) FC 3, 6, 16
- 2) Make FC04 look like 3 (but not sure the value of FC04)
- 3) Assuming all bits are READABLE via FN 03, then you don't really need FN 1 & 2. I can't think of any normal client/host which could NOT handle bits returned as packed blocks of 16 in holding registers.
- 4) You could still do FN 05 to write a single bit, as it is hard to do bit writes via the FN16 since you'd over-write 15 bits to write 1.

5) You could do FC15, but then you are back to needing bit-shifts. If they are easy to do fine, otherwise skip the hassle.

Luca Gallina shared more information about his project:

Thank you for replies and opinions.

1. Yes, I'm doing the RTU flavor.
2. My aim is to sell the S7 blocks as communication libraries.

I haven't planned a TCP driver since I suppose it's fairly simple to send Modbus PDUs over Ethernet. Most of the people seem to have difficulties in creating the S7 code for generating the CRC used in serial Modbus communication.

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

- Interactivity
- Knowledge aggregation
- Contact with other Modbus users

Discussion supported by...



More from the Modbus Discussion Forum...

Most used Modbus Functions, *cont'd...*

Do you think it would be interesting (read: worthwhile) to develop also a TCP version?

M Griffin answered:

I am assuming a TCP version would be worthwhile based on the number of questions we see on this list concerning how to connect a Siemens PLC to another brand via Ethernet.

Ethernet seems to have become popular for supervisory networks and Modbus TCP seems to be the closest thing there is in PLCs to a common protocol that most PLCs can use one way or another.

Typical uses would be:

1. Connect a Siemens PLC to another brand via Ethernet.
2. Connect a Siemens PLC to a SCADA or HMI system when there is a mix of different PLCs in the system.
3. Connect a Siemens PLC to a PC where Profinet isn't a desirable option (e.g., due to driver compatibility or integration problems).

As for whether it is easy for people to create their own Modbus TCP messages, it's "easy" if you have read and understand the spec. in detail. It's not easy if you've never done it before. Have a look at the typical questions we get here about Modbus. I suspect that the majority of PLC users don't want to know anything about protocols and would rather just use an off-the-shelf driver.

If you are offering an RTU version as a cheaper alternative to

loadable drivers, then I assume you could offer a TCP version for a similar purpose. I haven't, however, investigated the details of how you would do this.

Siemens has a Modbus TCP driver for their PLCs .

They have two versions that support functions 1, 2, 3, 4, 5, 6, 15 and 16, and another version that supports 3, 4 and 16. They do client and server. (I'm mentioning this because it relates to your original question).

[Read more or add your comments to this thread.](#)

Changing the Port Number of a Modbus TCP Device...

Nizar asked the forum:

I want to know whether we can change the port number of a Modbus TCP device from 502 to some other or if it can't be changed.

M Griffin's insight :

Port 502 isn't in the actual Modbus TCP protocol messages. However, it is what TCP/IP uses to tell the operating system (or firmware) at the destination which program to deliver the message to when it gets there (UDP/IP works exactly the same way). TCP/IP is like the address of an apartment building, while the port number is like the number of the apartment in the building.

You can change the port number, provided both ends of the connection know about the change, and provided the software allows you to make the change.

When Modbus was made to run on Ethernet, someone thought that 502 was a good convention for everyone to use so that you wouldn't have to set the port number as well as the IP number. A lot of software, however, may simply have hard coded that number in instead of making it an option that you can change.

If you are running the Modbus TCP server on a PC, you may be able to re-map the port numbers so that it looks like one number from the outside, while the program itself is running a different port number. I can tell you how to do this with a Linux OS. I don't know if MS Windows (if you are using that) has that capability, however.

Mark said:

The specification states port 502 for connectivity between Modbus TCP clients and server.

If you deviate from the specification by changing port number, all clients would need the capability of using an alternate port number.

Sometimes, it's necessary to run multiple servers from a single IP address, so we provide a provision in all of our Modbus TCP client and server products to change port number.

For proprietary applications, there should be no problem using an alternate port number, as long as clients and server have that provision. If you are building a commercial product, you should default to 502, but might want to build in the capability to specify an alternate port.

[Add your comments to this thread.](#)

We're with you. The Modbus Organization is there to help suppliers and users of the Modbus protocol succeed. Our members range from Modbus device suppliers, 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.

Designing with Modbus

Modbus developers rely on the Modbus Organization for valued assistance with their projects:

- Start by downloading specifications and other design documents from the modbus.org website.
- To save time, [purchase the Modbus TCP Toolkit](#) CD (FREE to general members); it contains source code and a myriad of other resources.
- If you come across technical issues that have you stumped, post your question on the [modbus.org forum](#). One of the many experienced Modbus implementers who frequent this forum will likely have your answer.

Conformance Testing

When your project's done, how do you know it really conforms to the Modbus specification? 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.

Then [submit your product for testing](#) to the Modbus Organization for conformance testing. 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.

Your company will 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?

Again, the [modbus.org forum](#) is ready to answer your questions and provide guidance. Thousands of users from diverse backgrounds participate in the forum, giving you a powerful base of experience from which to draw.

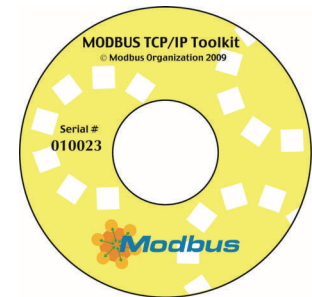
The Future is Yours

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.

[Download the Modbus Organization Membership Application](#) to learn about the different membership levels and their associated benefits.

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. The toolkit contains the following items:

Modbus Documentation

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

Tools

- Modbus TCP Client & 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

Modbus Conformance Testing

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

Additional Resources