

### WCT Makes Modbus Mapping Progress

The Modbus Subcommittee of the Wireless Cooperation Team (WCT) continues to work on the project and has made strides in conceptualizing the gateway parameters. Committee members have made some initial decisions to design a gateway specification that will be as straightforward and simple as possible.

Look for regular updates on the gateway specification development over the coming year.

### Welcome to New Members!

- Advanced Micro Controls Inc (AMCI)
- Bentek Systems Ltd.
- Define Instruments
- Domat Control System s.r.o.
- Trebing & Himstedt Prozeßautomation



### Blog Focuses on Security

Modbus Organization member company Byres Security (a Belden company) last week reported on a hacker who showed how he could easily hack into a SCADA system controlling the water utility in the City of South Houston.

In [this blog entry](#), Eric Byres discusses the vulnerability of passwords and the inherent risk password protection poses to critical systems. With tips for choosing "memorable yet effective" passwords, there's good advice here for everyone.

### Modbus Device Directory Expanding

The Modbus Organization has maintained a directory of Modbus products — hardware devices and software programs — since launching its current website in 2008. Today there are almost 1200 listings, affording users the ability to search for products for their projects based on a variety of criteria.

Recent entries include an increase in the number of wireless devices, well as the number of devices and programs focusing on energy management.

The directory lists Modbus Conformance-tested devices first, followed by member companies' products. Non-member listings are also included, but do not include either spec. sheets or links.

[Contact us](#) to inquire about adding your company's Modbus products to the directory or how to find the right Modbus device for your application.



**Advanced Micro Controls Inc (AMCI)** is a U.S.-based manufacturer with a global presence. Its industrial controls are sold all over the world, including eight different product families: Stepper Motor Controls, PLC Modules, Rotary Sensors, Networked Devices, Standalone Solutions, Packaging Systems Controls, and Stamping Press Technologies.

Founded in 1985, AMCI leverages an international network of distributors, so customers can quickly and conveniently purchase products, no matter where in the world they are located.

In May, AMCI announced Modbus TCP support for the company's robust NR25 series encoders.

**Trebing + Himstedt** is an international supplier of products and services for the optimal use of IT in the production environment. The company supports customers in their manufacturing processes, allowing targeted access to



production and process information through continuous integration across different communication levels – from the automation level to the ERP system.

In its Industrial Communication business unit, Trebing + Himstedt's products ensure the availability of industrial networks. The Manufacturing Integration business unit encompasses solutions for production IT, particularly for Manufacturing Execution Systems in SAP environments.

**Bentek Systems**, based in Calgary, Canada, is a company dedicated to the design and manufacture of industrial



wireless SCADA and telemetry solutions. The company provides products and services to industries including oil and gas, water and wastewater, mining and manufacturing.

SCADALink is Bentek Systems' own line of SCADA & automation products. The SCADALink line includes integrated RTU/Radiomodems, cellular- and Internet-enabled RTU/Radiomodems, wireless Ethernet radios, serial Ethernet gateways, wireless I/O telemetry, solar-powered RTU systems, alarm callout systems, and protocol converters.



### 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](http://www.modbus.org)

Newsletter Editor:  
Lenore Tracey  
(lenore@modbus.org)

Copyright 2011  
Modbus Organization, Inc.

## Reliability: High and Costs: Low

For a wastewater treatment plant, reliability is of great importance. The removal of wastewater and stormwater in extreme situations must happen when required. Costs are also important, and the key is to ensure cost-effectiveness without compromising the reliability and sustainability of the wastewater treatment plant.

At Bjerringbro Wastewater Treatment Plant in Denmark, data registered by Dedicated Controls is effectively transmitted wirelessly via a CIM 250 communication interface module. This has reduced the need for manual inspection, improved preventive maintenance and ensured reliability of the wastewater facility.

Bjerringbro is located in mid-Jutland, Denmark. The Bjerringbro Wastewater Treatment Plant is one of 22 wastewater treatment plants serving 250 pumping stations operated by Energi Viborg. Bjerringbro Wastewater Treatment Plant has 35 pumping stations, four of which run Grundfos pumps transmitting data wirelessly via CIM 250.

### The Situation

Prior to the installation of the wireless solution at the pumping stations connected to the Bjerringbro Wastewater Treatment Plant, manual inspections were necessary on a weekly basis for local pumping stations and daily for main pumping stations, to ensure correct operation and to detect possible faults. This required that staff be present at the treatment plant every day of the week, all year round.

Previously, the warning system at one of the local pumping stations consisted of a lamp placed high up on a lamppost; and reaction to a warning depended on the lamp being seen and reported! Today, wireless transmission sends the full register of pump pit activity every ten minutes to the SCADA system at Bjerringbro Wastewater Treatment Plant.

### The Grundfos solution

Using the terrain cabinet at the Engvej Øst local pumping station as an example, the robust cabinet includes a meter and a sewage pump controller (Dedicated Controls) with a CIM 250 module that has a GSM/ GPRS modem with its own IP address and mobile phone number. The use of a SIM card to establish the wireless connection makes installation easy, as the GSM/GPRS operator delivers the communication infrastructure.

*“Wireless transmission means we get data here and now – and that’s data we can use,”* says Kaj Lorenzen, Driftsleder, Bjerringbro Renseanlæg.

Data is communicated wirelessly every 10 minutes to the central SCADA system. In an alarm situation, the SCADA system ensures correct alarm handling.



*Sewage pump controller with a CIM 250 module and GSM/ GPRS modem are to the right.*

Winpacer software – a log program for SCADA on the computer at the treatment plant – sets the schedule, ensuring the alarm is sent to the correct personnel at the right time, according to five pre-determined levels of alarm situations and response times.

The data transmitted includes the main status of the pump pit and pumps and users can request active alarms and warnings.

The types of alarms include sewage overflow, low flow, dry running, under-voltage, blocked motor/pump, over-temperature, and others that can be adapted according to the user's needs.

Currently, there are about 200 of these cabinets installed in Denmark with Dedicated Controls transmitting wirelessly via the CIM 250 module.

## Wireless Water...

*cont'd from pg 3*

### The Outcome

The immediate benefits of the wireless communication offered by the CIM 250 arise from the system showing how a pumping station is running over an entire day. This helps save time and money by reducing the need for manual inspections and helping make better planning possible. In time, this means greater reliability from better preventive maintenance.



Personnel only get called out if absolutely necessary and they can act earlier. In addition, the wireless system provides operational data for control and statistics. This increases the possibility of even greater measures for ensuring maintenance planning, operational reliability, and also for optimising efficiency in the future, because all data is saved in a database.

## Advertise on the Modbus.org Website

With a **half million pages served to almost 30,000 unique visitors each month**, what better place to advertise your Modbus devices and software?

[Contact us](#) for a rate sheet. A special member's discount makes banner advertising an even better deal when you join the Modbus Organization.

## Control Announces Modbus Router

**Control Corporation** announced Modbus Router, the latest firmware application for its DeviceMaster UP Industrial Gateway family of products. The Modbus Router firmware was developed to provide network-wide Modbus connectivity between a wide variety of Modbus masters and local and remote Modbus slaves. Modbus Router provides a highly flexible and easy-to-use connectivity solution.

What can Modbus Router do?

- Simultaneously connect up to 123 Modbus masters to as many as 255 Modbus slave device(s)
- Automatically detect local slave devices and route messages
- Connect serial Modbus masters to Modbus TCP networks and remote Modbus slave devices
- Convert Modbus protocols, such as Modbus/TCP to Modbus RTU/ASCII
- Deliver diagnostics and status pages to enhance maintenance and problem-solving capabilities
- Solve common problems such as relocating devices or connecting additional Modbus masters to an existing installation

See [Control's Modbus Solutions web page](#) for more info.



## Two-port version of Anybus CompactCom

**HMS Network's** two-port version of Anybus CompactCom for Modbus TCP is a fast and easy way for industrial device manufacturers to achieve connectivity to Modbus TCP. It also reduces the need for expensive external switches and cuts down on factory wiring since the module comes with a built-in switch of its own.

The new two-port Modbus TCP module includes an integrated switch that makes it possible to build networks in normal field-bus style (daisy chain) rather than connecting all devices through an external switch. This reduces the need for expensive external switches.



The [Anybus CompactCom](#) module acts as a slave on the Modbus TCP network. It is available with and without housing and is about the size of a compact flash card. The core of the module is composed of HMS's NP30 microprocessor with its integrated fast Ethernet controller along with RAM and Flash memory for the Modbus TCP device software stack.

## Q&A from the Modbus Discussion Forum...

### Modbus writing 16-bit signed (-) values

#### neilrudds asked:

Hi, I'm new to the forum and quite new to the Modbus protocol and I'm hoping someone can help me with my Modbus problem.

I am using RS485 to communicate with a generator engine controller. The controller stores a series of event records across several string type registers that contain firstly date, time and event log reason; secondly the state of all inputs/outputs of the engine (this works well and is not the issue).

The issue is:

To acquire this data I must first write to a 16-bit signed register the actual ID of the event record before I can read out the data. The record ID's range from 0 to approx. -1200 depending on the records logged.

I have had success writing from 0 to -128 and the correct records are then contained in the appropriate registers, but after -128, I have many problems. For example, when trying to write -384, I am actually given record -128 but -385 is ok and gives me the correct record. And again writing -256 give me -256 but -257 gives me -1. I have looked at the binary values etc. and cannot see a problem.

Any help is greatly appreciated!

#### Rob replied :

It sounds like something somewhere is getting 8-bit and 16-bit words confused.

8-bit signed numbers range from -127 to +128

16-bit signed numbers range from -32766 to +32767

If you are familiar with the "2s Compliment" notation you will understand how negative numbers are encoded - i.e. if the MSB is SET then the number is negative. [http://en.wikipedia.org/wiki/Two%27s\\_complement](http://en.wikipedia.org/wiki/Two%27s_complement).

In your case it appears that when you write a value where bit 8 is set (i.e. the MSB of an 8-bit word) it will appear as a negative integer value. I suspect from your symptoms that you are either writing 8-bit words or your device is expecting 8 bits instead of 16.

#### Lynn Linse suggested:

This isn't really a Modbus problem as Modbus literally moves all registers as 'unsigned 16-bit'. Modbus is the delivery truck & doesn't care what's in the package.

The problem is in how your code is packing your signed integer into that unsigned 16-bit word.

Your signed INT is likely 32-bit if a PC or modern embedded system, but perhaps 8-bit if your system is trying to highly minimize data memory usage.

Since a PC is also little-byte first and Modbus is big-byte first, this makes packing a signed integer from 'host form' to 'Modbus form' tricky.

I can't explain how you accomplish this, but since the most common design is something like:

```
modbus[0] = (X >> 8) AND 0xFF
modbus[1] = (X AND 0xFF)
```

Your symptom sounds like your first equation is always resulting in 0xFF. The shift-right (>>) operation may have unexpected consequences on a signed integer in some systems.

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

#### [The Modbus Community](#)

- Active technical discussions
- Knowledge aggregation
- Contact with other Modbus users

Discussion supported by...

**control.com**<sup>®</sup>

## Modbus and SCADA...

### Yes 123 wrote:

I am new to SCADA systems. Recently I was going through some Modbus TCP-related documents.

My question is: If I write a C++ application that makes a PC behave as a Modbus TCP slave, then how can I write data to memory/registers so that a Modbus TCP master can read that?

### Mark offered:

Check out [automatedsolutions.com](http://automatedsolutions.com) for a Modbus TCP Server (Slave) ActiveX Control that handles all the Modbus stuff for you and provides a simple API for read/write access to Modbus registers.

<http://automatedsolutions.com/products/modbusslave.asp>

-Mark ([automatedsolutions.com](http://automatedsolutions.com))

### Dixit suggested:

It depends on the way you are going to use/develop the SCADA system.

I make my SCADA applications using .NET platform and use the

communication drivers from [www.Parijat.com](http://www.Parijat.com). Those drivers are based on .NET technology, so no extra software installation needed.

I [have used] their Modbus TCP Slave as well Master drivers from many years.

They also provide demo application, so you can test your Master application with their PC resident Modbus TCP Slave driver.

### Lynn Linse's advice:

If your goal is to learn Modbus, this is fine and can work.

If your goal is just testing your SCADA, then you will find many free (or nearly-free) Modbus TCP slave "simulators" online. Just search for "modbus slave simulator" and you'll find them.

Also, if you plan to do any TCP programming, make sure you have Wireshark (free/open-source at source-force) or some other tool which can decode Modbus/TCP over the wire.

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

## Questions? Comments? Need Help?

The Modbus discussion forum offers users and developers the opportunity to ask and answer questions about Modbus communications and applications. [Post a message](#) and your peers can offer their opinions and expertise to help you solve a problem, understand a principle, or debate the conventional wisdom.



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](http://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.

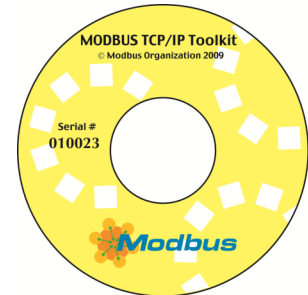
## The Future is Yours

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