Why Can't We Be Friends?
Monitoring the Server Room by Introducing Modbus to SNMP

Stanley Liu

Product Manager, Data Acquisition & Control Division

Overview

IA devices are very useful for monitoring server rooms in IT systems, but the right integration solution is required to make this unlikely pairing of different technologies seamless and effective.

Industrial Automation (IA) devices can dramatically improve server room monitoring and reduce system downtime. Unfortunately, introducing new devices into an existing system is never easy. This challenge is only complicated when the new devices use an alternative communications protocol, or are from a completely different family of technologies altogether. Despite these obstacles, IT departments are increasingly discovering that they would like to be able to deploy and monitor IA devices, such as UPS and battery equipment, temperature and humidity sensors, power consumption meters, data switches, or even live video, in their server rooms. However, IA devices typically use a Supervisory Control and Data Acquisition (SCADA) protocol, such as Modbus. This is new territory for IT professionals, who are more familiar with using Network Management System (NMS) tools and Simple Network Management Protocol (SNMP) with Ethernet networks. Without an integration solution, IT personnel would need to master a completely different IA skill set to add these devices to their existing NMS.

On the face of it, IA's SCADA/Modbus devices and IT's NMS/SNMP systems seem to be wholly incompatible—but sometimes, all that's needed is a mutual friend to help bring two opposites together. This white paper will explore how

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com

MOXA®

This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

selecting the correct solution allows existing IT departments to easily deploy and monitor the full range of available IA devices for server room monitoring, without complicated integration obstacles or additional training requirements.

Benefits and Limitations of IT Network Management Systems

It would be ideal if organizations could leverage their existing IT assets to manage the many useful devices that traditionally fall in the IA category.

The value of using computer networking is well-established in today's business environment, and because of this most organizations possess some institutional familiarity with IT technologies, such as Ethernet, SNMP and NMS. Correspondingly, the supply of IT expertise is also high, so organizations that wish to improve their IT capabilities find that it is not difficult to do so. It makes sense to build on this existing expertise with IT tools and protocols by employing them wherever possible.

SNMP technology is commonly used with NMS as it is a reliable, scalable, and straightforward way to monitor the conditions of devices attached to a network. This IP-based technology uses a simple and cost-effective Manager-Agent model to enable remote access and monitoring over the Internet or an intranet, while avoiding physical and geographical limitations.

However, NMS administrators are beginning to find that their systems could be much more effective and reliable with the addition of devices beyond those commonly accessible via SNMP. Devices such as environmental sensors, power regulators, or video cameras can dramatically increase an NMS's ability to monitor network conditions. Unfortunately, these devices are commonly SCADA devices that use Modbus, which is a completely different protocol from SNMP. Deploying these devices usually requires familiarity with industrial automation (IA). Previously, complex and costly middleware as well as additional training and development were required to combine IA and IT components.

Middleware—an Imperfect Solution

Middleware is one way to combine SNMP and Modbus devices on one network, but it is a complex and costly undertaking that involves a complete system overhaul.

Mixing IA and IT components on one network can be so advantageous that administrators trying to do so are willing to make significant compromises and deploy middleware. In the middleware approach, administrators first convert their NMS into a SCADA system, allowing the use of the new Modbus devices. A SNMP OPC server is then installed to collect data from existing SNMP devices and display it on the SCADA system. This SNMP OPC server acts as "middleware" between SNMP network devices and the SCADA system.
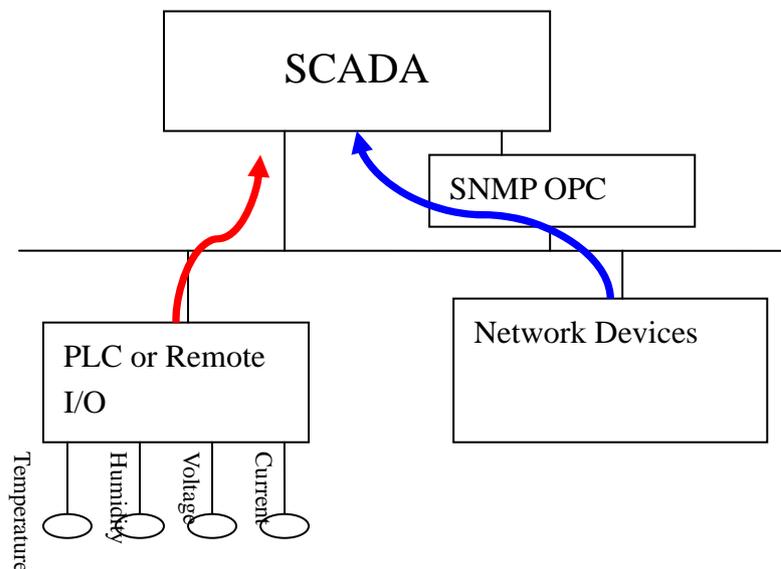

Figure 1: The Middleware Solution. The system has been overhauled to use SCADA.

This strategy represents nothing less than a complete overhaul from one system architecture to another. While such a strategy does succeed in connecting the new devices, the costs and challenges of attempting a radical system rebuild such as this are self-evident. Administrators will need to learn how to operate a SCADA system, which is a completely different animal from the IT networks they are accustomed to maintaining. All the investments in NMS and SNMP training and products that have already been made must be discarded. It is

a testament to just how useful Modbus devices can be that IT departments would even consider such a drastic solution. It would be far better to find a solution that is easier to implement, interoperable with the existing NMS architecture, and free from costly complications.

Bridging IA and IT with Intelligent Ethernet I/O

A better solution would be to find an I/O device that has both Modbus and Ethernet support. This device should have local intelligence and high security, yet remain simple to deploy.

An Ethernet device that communicates with the NMS system using SNMP, yet also manages inputs and outputs in the Modbus protocol, would be ideal for introducing IA devices to an existing NMS system. The overall system architecture would remain unchanged, and IT administrators can continue to use the NMS skills and tools they've already acquired. This I/O device would simply be another Ethernet device on the network.
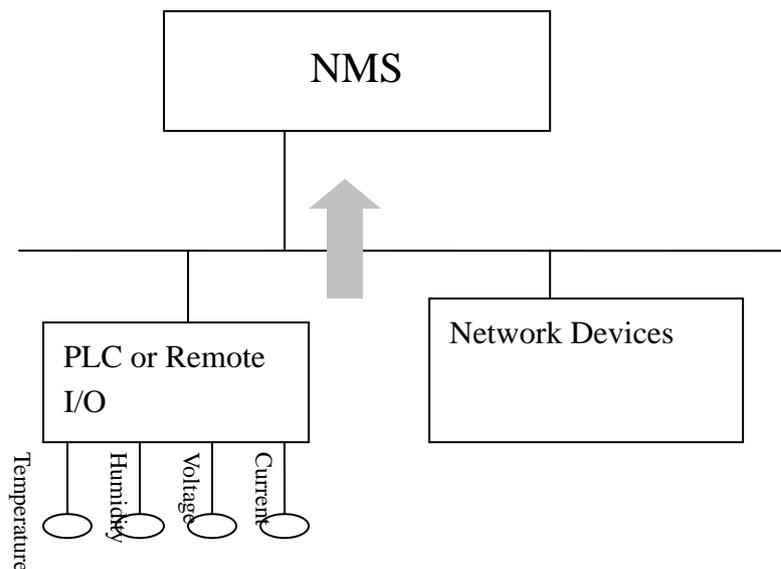

Figure 2: Intelligent Ethernet I/O Solution. The existing NMS architecture is maintained.

An ideal Ethernet I/O device would also be intelligent, meaning it can manage connected devices, replacing the need for a separate PC or PLC. This intelligence should extend to network communications, so that the device is smart enough to recognize which data is important and should be sent to the

host computer. Compared to a device that simply responds at a fixed interval, this would both conserve bandwidth and ensure that critical data is sent immediately. Network security features are also an important consideration as IT networks tend to be more vulnerable to hackers than SCADA networks, especially if the packets are routed over the Internet. At the same time, the I/O device must not fall into the trap of being feature-rich but too complex and time-consuming to deploy.

Moxa's ioLogik Products: Seamlessly Pairing IA and IT

Moxa's SNMP ioLogik products are perfect matchmakers for pairing Modbus devices to SNMP networks. They are efficient, secure, and easy-to-use.

Moxa's line of SNMP ioLogik products, such as the Ethernet ioLogik E2000 series, the modular Ethernet ioLogik E4200, and the cellular ioLogik W5340, offer a powerful yet easy-to-use IA-to-IT solution. These ioLogik products support all versions of the SNMP protocol, allowing hassle-free expansion of existing systems. Furthermore, Moxa's ioLogik products can deliver the following additional benefits:

- **Efficient and Precise Network Use**

Standard SNMP communications are governed by a Manager-Agent polling model in which the manager "polls," or sends a request, to the agent, which then returns a response. Moxa's ioLogik products can forgo this polling and be configured to send SNMP trap packets in a set interval, or when triggered by predefined events. This approach ensures that administrators are instantly notified of any critical events while remaining far more bandwidth efficient than polling.

The traditional disadvantage of using SNMP traps is the limited information that can be conveyed. There are only 7 standard trap numbers available in SNMP, so it can be difficult to tell what is happening just by looking at a list of traps. Moxa's proprietary SNMP trap format allows variable binding, which mitigates this disadvantage by adding more information to each SNMP trap. For example, an SNMP trap that triggers when the door sensor is tripped can include the message "Door Open."

- **Secure Private Communications**

Moxa's SNMP ioLogik products support all versions of SNMP, including SNMP v3. In fact, Moxa was the first solution provider to support SNMP v3 in an I/O product. SNMP v3 support is particularly essential because it introduced important security features that protect your network communications from unauthorized access. These include message integrity to verify that the packet contents have not been altered, authentication to verify that the packet comes from an authorized source, and encryption to ensure any packets intercepted by unauthorized machines are unreadable.
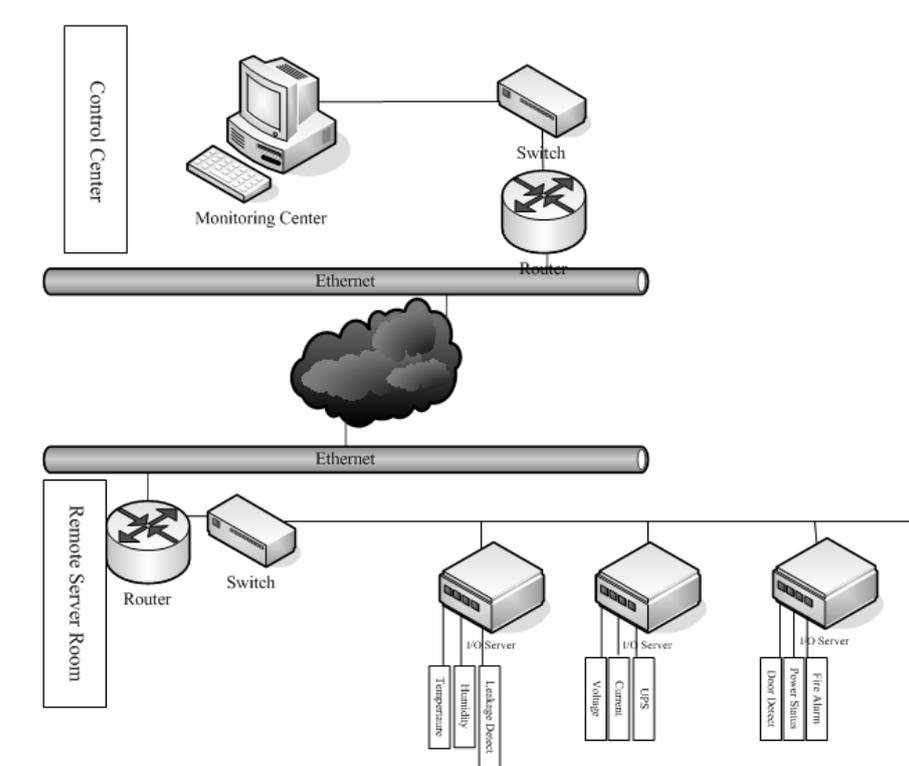

Figure 3: Moxa's Ethernet ioLogik device is simply another device on the Ethernet network.

- **Simple Yet Powerful Customization Options**

Moxa's Click&Go™ control logic grants administrators unparalleled control over the behavior of their I/O device, without involving third-party development tools or complex code. ioLogik products offer PLC-grade control, a timer,

scheduling, and register functions. Various user-defined events can be configured to send time-stamped TCP/UDP messages, emails, and SMS messages in addition to SNMP traps. The I/O device can even be further fine-tuned to include triggered timers, CGI commands, or remote actions. All of this local intelligence remains easy-to-manage using the simple and intuitive menu-driven Click&Go™ interface. Anyone familiar with basic IF-THEN-ELSE statements can configure the ioLogik. This combination of powerful, customizable features with simple development dramatically reduces deployment time without compromising on system capabilities.

A Seamless Partnership between IT and IA

With the right solution, the IT world of SNMP and Ethernet does not need to be inaccessible to IA modbus devices. To learn more about the ioLogik E2000 series, the ioLogik W5340, or the ioLogik E4200, or to order evaluation units online, visit www.moxa.com.