Remote Automation and Monitoring: PLC or RTU?

Introduction

Much has been written on the "PLC vs. RTU" subject. PLC suppliers produce application notes that say a PLC can be used as an RTU. RTU suppliers produce white papers that say an RTU is everything a PLC is and more. Both points-of-view are in need of a reality check.

This white paper focuses on automation and monitoring applications at remote locations and is intended to treat the "PLC vs. RTU" aspect as realistically as possible.

Background

What is the difference between a PLC and an RTU? In today's markets, broad product ranges make it difficult to generalize about either one.

We do know, at least, that PLCs and RTUs are similar devices but with somewhat differing functionality. PLC and RTU product lines include "bricks" for small applications and modular versions for larger applications. A comparison of I/O hardware reveals mostly similarities. The same is true for programming languages. While ladder logic is fundamental to a PLC, many RTUs can also be programmed using ladder. Many PLC and RTU products can further be programmed using any of five languages in the industry-standard, IEC 61131-3 suite. Communications similarities include Ethernet, RS-232 and RS-485 interfaces while USB connections are becoming increasingly popular.

The differences come down to economics.

PLCs are designed to address plant-floor, programmable automation applications. These applications comprise a very large market, into which PLC manufacturers have shipped millions of units. For PLC designs, wide area, SCADA networks and remote site installations are low on the priority list because those markets are much smaller.

On the other hand, RTU manufacturers target the wide area, SCADA applications at remote sites and avoid competition with PLCs for plant-floor, programmable automation applications. How the RTU manufacturers found themselves addressing the smaller markets is generally a matter of history, which has resulted in core competencies that make continued pursuit of them the best, economic decision.

Priorities Drive Designs

Traditionally, the design priority for a PLC is scanning I/O and executing ladder logic as quickly and as cost-effectively as possible. In today's systems, networking has also emerged as a key requirement. With their designs driven by plant floor applications, PLCs are best suited to wired, high-speed networks.

The fact that many RTUs use ladder logic implies that scanning and executing priorities are the same as they are in PLCs. However, communications take on a much higher priority in RTUs. RTUs are more effective in wireless, wide area network applications and operate well on both high-speed and low-speed networks.

Network speed is a generalization worthy of clarification. Definitions, today, range, widely, 300 – 115K baud for "low-speed" and above 115K baud for "high-speed." Note that baud rates of 9600 and 19,200 are still common for low-speed networks while 10/100M baud Ethernet is common for high-speed networks.

Emphasizing communications, RTU designs generally use multitasking kernals, which allocate CPU time between scanning, programmable logic execution and communications. Most PLC designs do not sacrifice I/O scanning and execution of ladder logic. For network communication operations, they employ coprocessors.

Among manufacturers of PLCs and RTUs, considerable R&D work has been invested in cost-effective firmware, hardware and software for their target, vertical market applications. An RTU manufacturer simply cannot make up for all the work PLC manufacturers have put into development of firmware/software functionality and numerous hardware modules for plant floor applications. Similarly, a PLC manufacturer cannot make up for all the work the RTU manufacturers have put into interfacing a broad array of communications hardware devices and implementing numerous, communications protocols for wide area SCADA networks.

Differentiators for Remote Automation and Monitoring

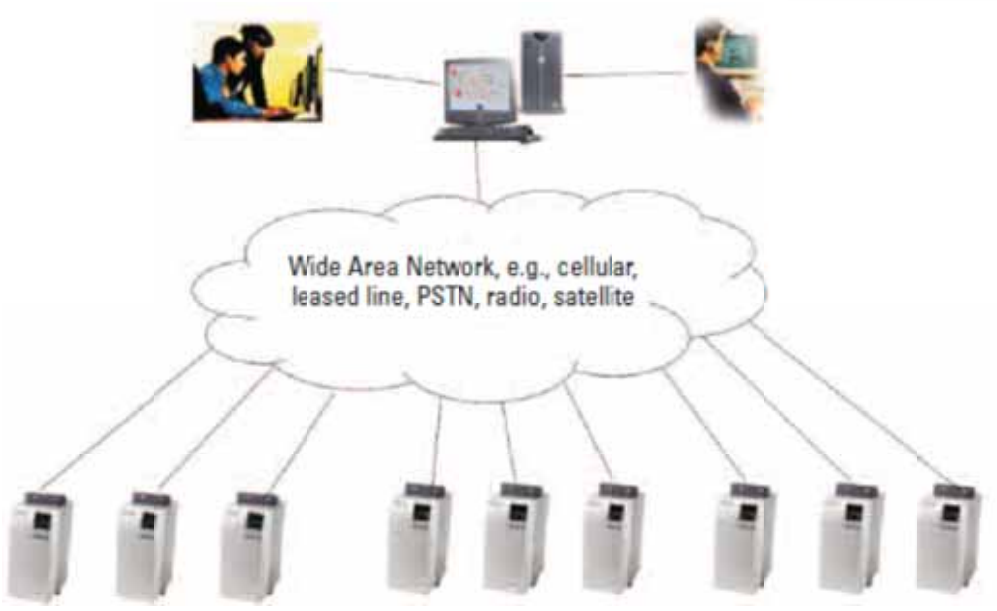
Through their millions of installations, PLCs are well understood by many people. When a remote automation or monitoring project comes along, many engineers will naturally attempt to apply a PLC.

The problem with remote applications is that they are not simply adaptations or extensions of plant floor applications. There are many, key characteristics that differentiate the requirements of remote automation and monitoring.

Two, fundamental issues with remote installations vs. plant floor installations are:

- Bandwidth comes at a cost.
- Installation comes at a cost.

Bandwidth cost affects PLCs much less so than RTUs. A PLC design assumes that a low-cost, reliable, high speed, local area network on the plant floor will provide rapid updates to HMI devices as well as to one or more servers, which perform alarm management, report generation, supervisory control, material tracking, production management and statistical quality control.



An RTU design must assume a less reliable, low speed network with a higher connection cost and higher, operating cost, all of which encourage the user to minimize the amount of data that is transferred over the network. This incurs more ramifications than engineers may, at first, consider.

An RTU must support not only a broad variety of communications hardware, network providers and protocols, it must further incorporate data handling functionality including alarm management, calculations such as for gas flow, and data logging. Since PLCs interface with SCADA servers via much more reliable, hard-wired, high speed networks, they can off-load alarming, calculation and historian functions to the servers.

Remote installations present hurdles that are not encountered on the plant floor. RTU designs must be hardened for electrical isolation, humidity, temperature extremes, and vibration conditions, which are unique to remote sites. In addition, many remote locations completely lack installation infrastructure and power.

Sites lacking power demand features such as low current draw for operation on batteries and solar power systems. Remote locations, of course, also introduce higher travel costs. RTU designs include measures to reduce the number of site visits required for operations and maintenance purposes. Let's look into these differentiators a little further.

Communications Hardware and Provider Network Compatibility

Available on today's market is a broad variety of wide area communications hardware and network service providers. While users are confronted with a considerable selection process, each network offers a feasible value proposition. In order to be relevant in the market, an RTU must be compatible with as many of them as possible.

Communications choices popular, today, include cellular provider networks, leased telephone lines, private radio networks, provider radio networks, public switched telephone networks (PSTN), and satellite provider networks.

When private radio emerged as an effective alternative to leased telephone lines, end users were compelled to weigh not only costs-of-purchase but also operations and maintenance costs vs. periodic costs of a third party provider network.

Radio transceivers, power sources, enclosures, antennas and towers illustrate the communication hardware costs that are well beyond those incurred on the plant floor. Bandwidth costs are illustrated by the facts that higher-speed radios are more expensive and bandwidth is inversely proportional to range. The latter could mean more repeaters and the infrastructure to support them in order to maintain performance over a long distance.

Licensed and unlicensed, spread spectrum radios are available, today, from numerous suppliers. Many RTU designs have tightly integrated multiple, board-level versions, which provide major savings over systems that interface with external, standard-model radios.

In addition, RTU manufacturers have done extensive testing with a large number of radios from many manufacturers and have incorporated a significant level of configuration and diagnostics capabilities into their software tools offerings. Such major investments in terms of R&D resources offer appreciable value to SCADA system engineers and users.

RTU manufacturers have also integrated provider network hardware and corresponding software tools. Most popular are cellular radios such as GSM/GPRS. While the hardware purchase cost is normally lower than it is for a radio, users pay for bandwidth on a monthly or annual basis.

Like integral, spread spectrum radios, integral GSM/GPRS cellular radios offer savings over external models. Since integral, cellular radios and spread spectrum radios are rare in PLCs, most PLC solutions must use external models at considerably higher cost. In addition, they lack the configuration and diagnostics tools, in which RTU manufacturers have invested so much experience. The result is significantly more project engineering time to realize a working system.

Communications Protocols for Wide Area SCADA Networks

Communications protocols for wide area networks differ from those used on the plant floor. Protocols such as DNP3, which is open architecture and in the public domain, include numerous features that apply specifically to the operation of SCADA systems.

If wide area networks offered the same economics, performance and reliability as local area networks, we wouldn't need protocols with all the capabilities included in DNP3. A basic list, provided by the DNP3 Users Group, includes the following:

- request and respond with multiple data types in single messages
- segment messages into multiple frames to ensure excellent error detection and recovery
- include only changed data in response messages (report-by-exception)
- assign priorities to data items and request data items periodically based on their priority
- respond without request (unsolicited)
- support time synchronization and a standard time format
- allow multiple masters and peer-to-peer operations
- allow user definable objects including file transfer

Provisions for error checking, link layer confirmation and message re-transmission allow reliable operation on less-than-reliable networks. Report-by-exception and unsolicited messaging minimize the amount of data transmitted over the network and help reduce costs in terms of bandwidth used.

A layered structure allows DNP3 to work in a broad variety of systems, including Ethernet, cellular provider networks such as GSM/GPRS, public switched telephone networks (PSTN), radio and satellite.

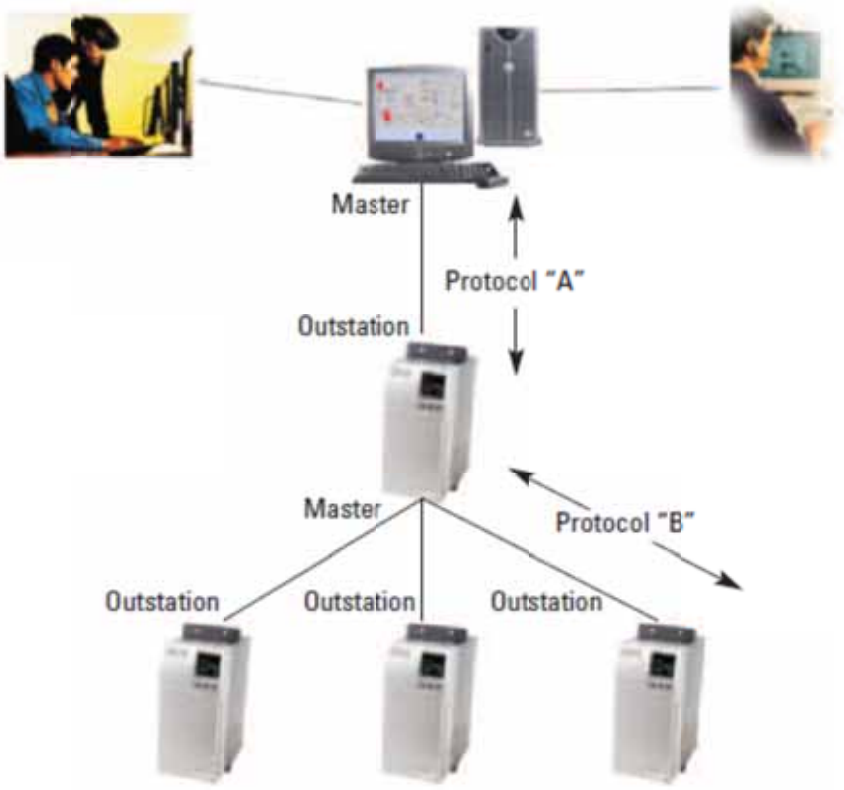
In addition to incorporating protocols, RTU manufacturers have made huge investments in intelligent network operations. For example, an RTU can perform dynamic message routing. An RTU is able to 'learn' about changes to network routing and respond by dynamically changing message routes. If primary communications are via radio communications on port 1 and messages have been failing, the master station may use an alternative communications path. If a new message from the master station is received on backup PSTN communications port 2, the RTU will change its routing information to reflect the fact that master station communications are now via port 2. Some RTUs can also re-direct messages based on success/failure statistics.

A major issue for RTU manufacturers is that even protocols with the capabilities of DNP3 have attained low market shares. In terms of communications protocols, the installed base is very broad and includes open standards, de facto standards and those that are vendor-proprietary.

Modbus, a de facto standard, is generally considered the leading protocol for SCADA systems. The fact that it is common in both PLCs and RTUs makes it unique. Modbus, however, is not dominant. That leads to the necessity for RTU manufacturers to offer literally dozens of protocols in order to adequately address the SCADA markets.

To extend data concentrator and protocol converter functionality to interface with PLCs, many RTUs have also incorporated some PLC-specific networks, such as DF1. But most RTU protocols are intended for use in wide area SCADA networks or with intelligent instrumentation, such as analyzers, field controllers, meters, sensor networks, etc.

Like the wide area network hardware, compatibility with SCADA protocols is a low priority for PLC designs — much like plant floor protocols are low priorities for RTU designs.



Alarm Management

Due to the reduced reliability of wide area networks as compared with plant floor networks, most RTU designs include significant, alarm management functionality at the local level. Not only does the RTU execute the logic to detect an alarm condition, it provides alarm notification over multiple networks and to multiple recipients.

When an RTU detects an alarm, it stores a time/date-stamped message in a buffer and maintains it until notification of the alarm is acknowledged. This ensures that no alarms are lost because of communications problems.

In addition to the SCADA protocol, notification messaging often can be via e-mail and SMS text. Text messaging usually allows the least cost in terms of bandwidth.

Using push (or, unsolicited) messaging, an RTU can immediately notify the SCADA master station of the alarm without having to wait for the next polling cycle.

Integrated alarm management includes control of repeated notification attempts, escalation, acknowledgement management and multiple levels of authority. Some RTUs even allow alarms to be acknowledged via a mobile phone.

Data Logging and Historian Functions

For reasons similar to those driving inclusion of alarm management, most RTUs provide historical data logging and event logging at the local level. In case of network problems, no data is lost. If the SCADA network is unavailable for an extended time, RTUs even allow for transfer of the data logs to a local PC, SD/MMC card or a USB stick.

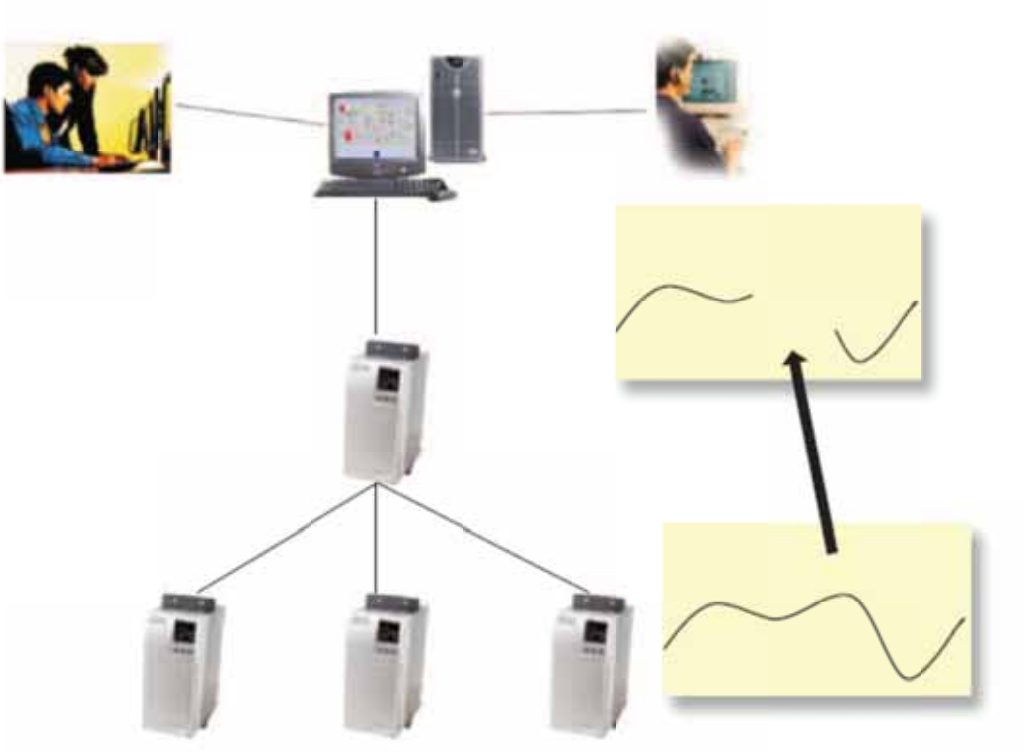
For a SCADA network in which bandwidth is at a premium, the local functionality significantly reduces data transfers. Instead of transferring every input sample over the network to a historian, the RTU locally maintains values such as averages and totals for time generations, including hourly, daily, etc.

Local data handling often extends to functions beyond data logging. For example, natural gas meter stations require the historical data logs to include not only averages and totals but also results of flow calculations per American Gas Association (AGA) reports. Instead of off-loading the AGA calculations to a server, the RTU includes that functionality in the firmware.

AGA calculations are not completely absent in the PLC world. Some PLCs do include them and, for a few other models, which do not, third-party modules provide the functionality — but at additional cost.

Sequence-of-events (SOE) logging is another function that is very common in RTU products. SOE is a virtual requirement for any product that is targeted to electrical transmission and distribution SCADA systems. In spite of their high-speed scanning capabilities, most PLCs do not provide the specific functionality that is required by the industry. SOE resolution is normally 1 millisecond and most RTUs include a high capacity for log entries.

Most RTUs, in fact, provide a high capacity, typically one Mbyte and often much higher, for storage of alarm messages, events and data logs with multiple provisions for data transfers. That capacity is uncommon in PLCs.



Remote Installation Design Requirements

Remote installation does come at a cost. Remote sites present a number of product design hurdles, which are unlike those on the plant floor.

Even when a PLC or RTU at a remote location is enclosed in a protective housing, it is still subject to outdoor, humidity and temperature conditions. Electronics, in particular, must be designed for wider ranges or the equipment could fail, sometimes in an unpredictable manner. A typical, temperature range specification for remote locations is -40 to 70 degrees C (-40 to 158 degrees F).

Since remote locations often lack infrastructure for equipment installation, PLCs can find themselves mounted in a manner that was not anticipated by the design team. RTU designers account for such circumstances and ensure that the product is rated for vibration due to installation nearby engines, pipelines, railroad tracks and other outdoor structures.

RTUs are also much more likely than PLCs to be offered with optional enclosures that are intended for outdoor installations. In order to protect against windblown dust and rain, the enclosures meet one or more Nema ratings, as used in North America and ingress protection (IP) ratings, as used in Europe. While a broad range of enclosures is available from third-party manufacturers, many RTU manufacturers have developed versions that are specific to their products and which are available at lower prices.

Remote sites are also often subject to problems with earth grounding. Electrical common mode rejection requires much higher isolation in the PLC or RTU. Ratings up to 3000Vdc are much more common in RTUs than in PLCs.

RTUs are also more often installed in areas in which a combustible gas or dust could be present in the atmosphere. Due to growing demand for automation and monitoring in the natural gas industry, PLCs have recently begun to gain ground in this area. Even though hazardous area ratings continue to be more common in RTUs, they no longer comprise the solid differentiator they once were.

Travel to remote sites comes at a cost. Large SCADA systems encompass thousands of locations spread over broad, geographical areas. Many sites are difficult to get to. Some systems must even be designed for the case that weather conditions prevent site visits for long time periods.

RTU designs include measures to remotely perform operation and maintenance functions in order to reduce travel costs and to continue functioning when sites are inaccessible.

An RTU is designed to operate as a “stand-alone” device. That is, there is no dependency on the communication network in order to continue all operations.

An RTU will report not only on the process but also equipment status at the site. Plenty of warning will be given before failure of key components such as batteries. RTU code includes asset management functionality that allows maintenance to be performed during the most optimal times in terms of site accessibility.

Some RTUs will use a separate protocol, such as SNMP, to transport information on system status while the primary protocol, e.g. DNP3, is used for process operations. While performing these functions, the RTU is well informed of the wide area network status and, if necessary, will use dynamic message routing to ensure delivery of information.

In the RTU configuration tools suite, most operations that are available to local technicians are replicated for use over the SCADA network. This allows those operations to be performed without the need for a site visit.

Such functionality on the wide area SCADA network puts more emphasis on security. RTUs are rising to that challenge by incorporating cyber security measures such as authentication and encryption. For example, DNP3 includes Secure Authentication using encrypted keys. Whenever a command is sent to an RTU over the network, the RTU can challenge the sending node to be sure it is a legitimate asset, such as the SCADA master station or a master RTU.

Low and Ultra-Low Power Consumption

RTUs are available in low and ultra-low power configurations that operate on batteries or solar power and extend the range of remote automation and monitoring to sites without any infrastructure. Generally, PLCs are not low power devices.

"Low power" defines a product that can operate on a small, solar power system using a panel rated, roughly, up to 30 watts and a lead acid cell battery up to 30 Ampere-hours (AH). "Ultra-low power" defines a product that can operate for a matter of years using internal batteries without a solar panel or other, charging source.

For locations that require the power source to be installed with the automation or monitoring device, low and ultra-low power designs can provide major savings on the order of hundreds of dollars per site.

Low and ultra-low power products use sophisticated designs that manage power to a number of platform subsystems. The most common trade-offs are communications availability and scanning performance. Since radio transmitters are typically the biggest power users, minimizing communications will maximize battery life. RTUs that use techniques including push technology via SMS text messaging and report-by-exception can provide process and site information whenever it is required while conserving power. Management of I/O scanning in a manner that is appropriate to remote processes such as tank levels can also conserve considerable power.

In these applications, the RTU must also report on the status of the power system, supervise temperature compensated, battery charging and further modify operations to conserve power if the battery is running low.

Conclusion

The differences between PLCs and RTUs come down to economics.

PLCs are designed to address plant-floor, programmable automation applications. These applications comprise a very large market, into which PLC manufacturers have shipped millions of units. For PLC designs, wide area, SCADA networks and remote site installations are low on the priority list because those markets are much smaller. On the other hand, the wide area SCADA applications at remote sites are core competencies and target markets for the RTU manufacturers.

Design priorities mean that PLCs include significant, plant floor functionality that is not included in RTUs. Similarly, RTUs include significant, wide area SCADA functionality that is not included in PLCs. For use in most, wide area SCADA systems and remote sites, an RTU will be more effective.

The RTU design is based on the higher bandwidth cost on wide area networks. The RTU will meet the requirements in terms of communication network interfaces, communication protocols and intelligent operation of wide area networks.

Since wide area networks are less reliable than plant floor networks, an RTU will include functionality that a PLC off-loads to a server on the plant floor network. Alarm management, historical data logging and flow calculations are features that RTUs include in order to be sure data is not lost because of communications problems.

RTUs designs are further hardened for installation in remote locations and two classes of product (low and ultra-low power) minimize current draw to cost effectively allow operation at locations that lack power sources.